Tivoli Identity Manager

Benutzerhandbuch

Version 4.5.0

SC12-3276-00

Tivoli Identity Manager

Benutzerhandbuch

Version 4.5.0

SC12-3276-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 43 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business Symbol ist eine Marke der International Business Machines Corporation
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle Java-basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Zweite Ausgabe (November 2003)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Tivoli Identity Manager End User Guide Version 4.5.0,
IBM Form SC32-1152-01,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2003
© Copyright IBM Deutschland GmbH 2003

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
November 2003

Inhaltsverzeichnis

Vorwort . . . . . **v**
Zielgruppe dieses Handbuchs v
Publikationen v
Tivoli Identity Manager Server-Bibliothek. v
Referenzliteratur vi
Onlinezugriff auf Publikationen. vi
Zugriffsmöglichkeit vi
Kontaktaufnahme mit der Softwareunterstützung vi
In diesem Handbuch verwendete Konventionen vii

Kapitel 1. Einführung **1**
Struktur von Tivoli Identity Manager 2
Navigation 3
Organisationsverwaltung 3
Personalverwaltung 3
Verwaltung von Services 4
Einrichtung 4

Kapitel 2. Anmeldung **5**
Auswahl der Sprache 5
Abrufen neuer Kennwörter 5
Kennwort vergessen (Kennwortprüffrage des Challenge/Response-Verfahrens) 6
Konfiguration des erzwungenen Challenge/Response-Verfahrens 7
Abrufen eines Kennworts 7
Erzwungene Änderung des Kennworts 8
Ablauf von Kennwörtern 8

Kapitel 3. Einheitliche Funktionen **9**
Navigation 9
Navigationsleiste des Hauptmenüs 9
Taskleiste 9
Gültigkeitsdatum 10
Hilfe. 10

Kapitel 4. Ausgangsposition **11**
Kennwortverwaltung 11
Accountverwaltung. 13
Hinzufügen neuer Accounts 14
Ändern vorhandener Accounts 15
Aussetzen von Accounts oder Zurücknehmen der Einrichtung von Accounts 16
Wiederherstellen von Accounts 16
Ändern von Kennwörtern 17
To Do-Liste 18
Anzeigen der Detailinformationen einer To-do-Liste 19
Anstehende Anforderungen 20
Beendete Anforderungen 20
Persönliche Informationen 20
Delegieren von Berechtigungen 22
Hinzufügen eines Stellvertreters 22
Wechseln des Stellvertreters 22
Ändern des ausgewählten Stellvertreters. 23
Antworten auf Kennwortprüffragen des Challenge/Response-Verfahrens 23

Kapitel 5. Berichte **25**

Berichtstypen 25
Berichte für Endbenutzer 27
Bericht ″Operation″ 27
Bericht ″Service″ 29
Bericht ″Benutzer″ 31
Bericht ″Zurückgewiesen″ 33
Bericht ″Datenabgleich″ 34
Bericht ″Ruhend″ 35
Bericht ″Account″ 36
Ad-hoc-Berichte (und Crystal Reports-Berichte) 38

Glossar 39

Bemerkungen 43
Marken 45

Index 47

Vorwort

IBM Tivoli Identity Manager Server (Tivoli Identity Manager Server) ist ein Verwaltungstool für die Verwaltung der Sicherheit in der gesamten Organisation. Dieses Handbuch erläutert die Verwendung der Endbenutzerfunktionen und Produktmerkmale von Tivoli Identity Manager.

Zielgruppe dieses Handbuchs

Dieses Handbuch wurde für Benutzer konzipiert, die für die Verwaltung ihrer Tivoli Identity Manager-Accounts verantwortlich sind. Bei den Lesern wird das Verständnis der grundlegenden Web- und Browserkonzepte vorausgesetzt. Darüber hinaus sollten die Leser in der Lage sein, Routinetasks auf Endbenutzerseite auszuführen.

Publikationen

Lesen Sie die Beschreibungen der Tivoli Identity Manager-Bibliothek, der Publikationen zu Produkten, die als Vorbedingung erforderlich sind, und der Referenzliteratur und bestimmen Sie so, welche Publikationen für Sie hilfreich sein könnten. Wenn Sie ermittelt haben, welche Publikationen Sie benötigen, folgen Sie den Anweisungen für den Onlinezugriff auf Publikationen.

Tivoli Identity Manager Server-Bibliothek

Die Tivoli Identity Manager-Bibliothek umfasst folgende Publikationen:

- Onlinebenutzerhilfe für Tivoli Identity Manager

  Stellt integrierte Themen der Onlinehilfe für alle Tivoli Identity Manager-Verwaltungstasks zur Verfügung.
- Separate Versionen des Tivoli Identity Manager Server-Installationshandbuchs für die Installation unter UNIX oder Windows mit WebSphere oder WebLogic. Verwenden Sie die für Ihren Standort relevante Version.

  Liefert Informationen zur Installation von Tivoli Identity Manager.
- *Tivoli Identity Manager Policy and Organization Administration Guide*

  Stellt Themen zu Tivoli Identity Manager-Verwaltungstasks zur Verfügung.
- *Tivoli Identity Manager Server Configuration Guide*

  Stellt Konfigurationsinformationen für Einzelserver- und Clusterkonfigurationen von Tivoli Identity Manager zur Verfügung.
- *Tivoli Identity Manager Benutzerhandbuch*

  Stellt Benutzerinformationen für die erstmalige Verwendung von Tivoli Identity Manager zur Verfügung.
- *Tivoli Identity Manager Server Release Notes*

  Stellt eine Zusammenfassung der Soft- und Hardwarevoraussatzungen für Tivoli Identity Manager zur Verfügung sowie Zusatzinformationen zu Programmkorrekturen (Fixes und Patches) und sonstige Informationen, die der Unterstützung dienen.
- *Tivoli Identity Manager Troubleshooting Guide*

  Stellt zusätzliche Informationen zur Fehlerbehebung für das Tivoli Identity Manager-Produkt zur Verfügung.

Referenzliteratur

Informationen im Zusammenhang mit Tivoli Identity Manager sind in den folgenden Publikationen verfügbar:

- Die Softwarebibliothek von Tivoli stellt eine Sammlung unterschiedlicher Tivoli-Publikationen wie White Papers, Datenblätter, Demonstrationen, Redbooks und Vertriebsfreigaben bereit. Die Softwarebibliothek von Tivoli steht auf der folgenden Website zur Verfügung:

  http://www.ibm.com/software/tivoli/library/
- Das Tivoli Software Glossary ist das Softwareglossar von Tivoli in englischer Sprache, das Definitionen für zahlreiche technische Termini im Zusammenhang mit Software von Tivoli enthält. Der Zugriff auf das *Tivoli Software Glossary*, das ausschließlich in englischer Sprache verfügbar ist, erfolgt über die Verknüpfung **Glossary** im linken Frame auf der Website ″Tivoli Software Library″ unter der folgenden URL-Adresse:

  http://www.ibm.com/software/tivoli/library/

Onlinezugriff auf Publikationen

Die Publikationen zu diesem Produkt sind online in der Softwarebibliothek von Tivoli in PDF-Format (Portable Document Format) und/oder in HTML-Format (Hypertext Markup Language) erhältlich:

http://www.ibm.com/software/tivoli/library/

Um Publikationen zu bestimmten Produkten in der Bibliothek zu finden, klicken Sie auf die Verknüpfung **Product manuals** im linken Frame auf der Website ″Tivoli Software Library″. Suchen Sie dann auf der Seite ″Tivoli Software Information Center″ den Namen des gewünschten Produkts und klicken Sie auf diesen Namen.

Die Produktpublikationen umfassen Release-Informationen, Installationshandbücher, Benutzerhandbücher, Administratorhandbücher und Referenzliteratur für Anwendungsentwickler.

Anmerkung: Damit PDF-Publikationen fehlerfrei gedruckt werden, sollten Sie in Adobe Acrobat im Fenster ″Drucken″ (**Datei > Drucken**) die Option **An Papierformat anpassen** auswählen.

Zugriffsmöglichkeit

Die Produktdokumentation umfasst folgende Funktionen, um den Zugriff auf die Publikationen zu erleichtern:

- Die Dokumentation steht sowohl im HTML- als auch im PDF-Format zur Verfügung, um Benutzer bestmöglich in die Lage zu versetzen, Sprachausgabeprogramme anzuwenden.
- Alle Grafiken stehen mit alternativem Text zur Verfügung, damit Benutzer mit Sehbehinderungen den Inhalt der Grafiken verstehen können.

Kontaktaufnahme mit der Softwareunterstützung

Bevor Sie wegen eines Problems Kontakt mit der IBM Tivoli-Softwareunterstützung aufnehmen, sollten Sie die Website von IBM Tivoli für Softwareunterstützung unter der folgenden Adresse prüfen:

http://www.ibm.com/software/sysmgmt/products/support/

Wenn Sie weiterführende Hilfe benötigen, kontaktieren Sie die Softwareunterstützung wie im *IBM Software Support Guide* auf der folgenden Website beschrieben:

http://techsupport.services.ibm.com/guides/handbook.html

Das Handbuch enthält die folgenden Informationen:

- Registrierungsbestimmungen und Voraussetzungen, die erfüllt werden müssen, um die Unterstützung in Anspruch nehmen zu können.
- Für das Land Ihres Standorts spezifische Telefonnummern und E-Mail-Adressen.
- Eine Liste der Informationen und Angaben, die Sie vor der Kontaktaufnahme mit der Kundenunterstützung zusammenstellen sollten.

In diesem Handbuch verwendete Konventionen

Dieses Referenzhandbuch verwendet mehrere Konventionen für besondere Termini und Aktionen sowie für betriebssystemspezifische Befehle und Pfade.

In diesem Handbuch wurden die folgenden Konventionen für das Schriftbild verwendet:

Fett **Fett** gedruckter Text weist auf auswählbare Schaltflächen in Fenstern sowie auf Einträge in Feldern und auf Befehle hin, die in diesem Handbuch verwendet werden. Eine Ausnahme hierzu bilden Beispiele oder der Inhalt von Dateien.

`Monospaceschrift`
Text in `Monospaceschrift` weist auf den Inhalt von Dateien, Dateinamen oder die Ausgabe von Befehlen hin.

Kursiv *Kursiv* gedruckter Text weist auf kontextspezifische Werte hin wie beispielsweise:

- Pfadnamen
- Dateinamen
- Benutzernamen
- Gruppennamen
- Systemparameter
- Umgebungsvariablen

% Das Prozentzeichen (%) weist auf die Eingabeaufforderung am Bildschirm durch die C-Shell als Teil der Beispiele hin, die in diesem Handbuch enthalten sind. Die Eingabeaufforderung am Bildschirm durch die C-Shell Ihres eigenen Systems kann hiervon abweichen.

Das Nummernzeichen (#) stellt die Eingabeaufforderung am Bildschirm dar, die Benutzern angezeigt wird, die als Superuser (Root-Zugriff) angemeldet sind.

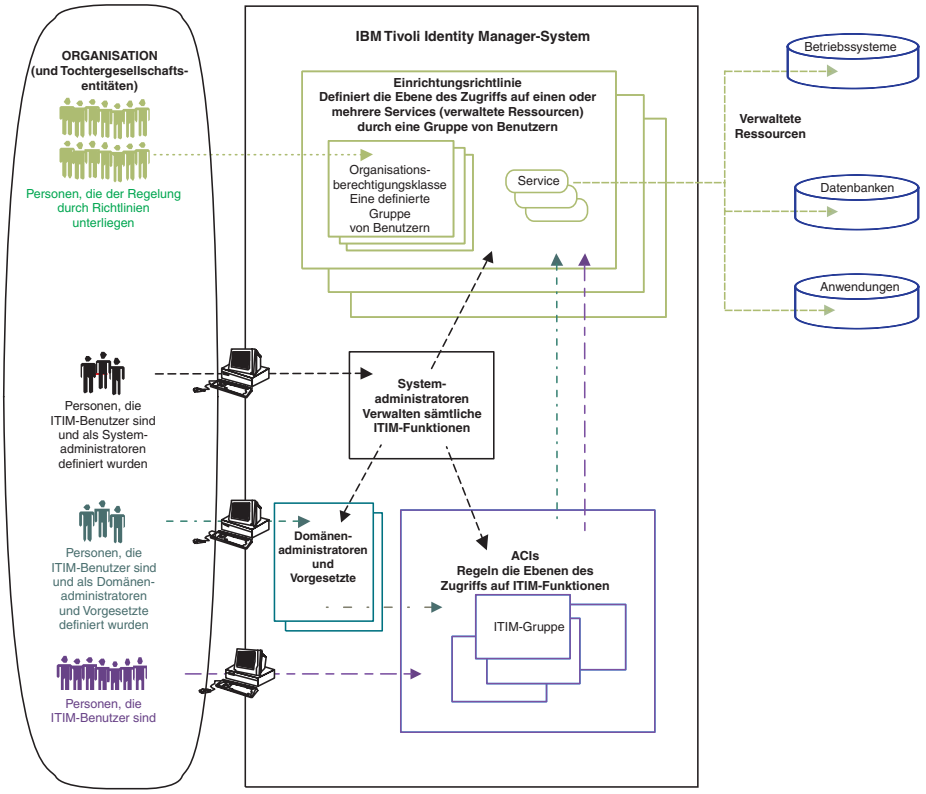
Kapitel 1. Einführung

IBM Tivoli Identity Manager stellt die erforderliche Software und erforderlichen Services zur Implementierung von richtlinienbasierten Einrichtungslösungen zur Verfügung. Tivoli Identity Manager unterstützt Unternehmen bei der Automatisierung der Prozesse, die notwenig sind, um Zugriffsberechtigungen für Mitarbeiter, Vertragsnehmer und Geschäftspartner einzurichten, damit diese auf die von ihnen benötigten Anwendungen zugreifen können. Hierbei spielt es keine Rolle, ob diese Zugriffsberechtigungen in einer geschlossenen Unternehmensumgebung oder in einem virtuellen bzw. erweiterten Unternehmen eingerichtet werden sollen.

Nach der Konfiguration von Organisationen und gegebenenfalls Tochtergesellschaftsentitäten, wie beispielsweise Organisationseinheiten, Geschäftspartnerorganisationen und Standorte, werden Personen hinzugefügt. Außerdem werden Organisationsberechtigungsklassen und ITIM-Gruppen erstellt. Die Personen können anschließend bestimmten Organisationsberechtigungsklassen und ITIM-Gruppen zugeordnet werden. Danach erstellen Sie Services, die den Zugriff auf die verschiedenen Typen verwalteter Ressourcen wie beispielsweise Oracle, Windows NT usw. ermöglichen. Organisationsberechtigungsklassen können über Einrichtungsrichtlinien miteinander verbunden werden und sind mit Services verknüpft, wodurch den Personen in den unterschiedlichen Organisationsberechtigungsklassen der Zugriff auf diejenige verwaltete Ressource gewährt wird, die mit dem betreffenden Service verknüpft ist. ITIM-Gruppen ermöglichen den Zugriff auf Tivoli Identity Manager Server. Die ihnen zugeordneten Berechtigungen in Tivoli Identity Manager werden durch sogenannte ACI (Access Control Information), d.h. Zugriffskontrollinformationen, erteilt. Durch die Zuordnung von Personen zu ITIM-Gruppen können diese Personen die erteilten Rechte in Anspruch nehmen.

Struktur von Tivoli Identity Manager

Nachstehend wird die Funktionsweise von Tivoli Identity Manager anhand einer Basisübersicht dargestellt.



Personen werden zu Organisationen und Entitäten hinzugefügt, die Tochtergesellschaften einer Organisation sind.

Eine Person kann einer Organisationsberechtigungsklasse zugeordnet werden, die ihr den Zugriff auf verwaltete Ressourcen erteilt. Die Erteilung des Zugriffs erfolgt anhand einer Einrichtungsrichtlinie, die die Berechtigungen festlegt, über die eine Person beim Zugreifen auf die verwaltete Zielressource verfügt.

Ein ITIM-Benutzer kann außerdem einer ITIM-Gruppe zugeordnet werden, die ihr Zugriff auf Tivoli Identity Manager Server erteilt. Die Erteilung des Zugriffs erfolgt anhand von Zugriffssteuerungsinformationen (ACI).

Einige Personen (in der Regel nur eine einzige Person oder zumindest wenige Personen) werden als Systemadministratoren definiert und haben auf allen Ebenen Zugriff auf sämtliche Funktionen von Tivoli Identity Manager.

Navigation

Die Navigationsleiste des Hauptmenüs am Anfang jeder Seite ermöglicht das einfache Navigieren im Tivoli Identity Manager-System. Um auf Funktionen der Optionen in der Navigationsleiste des Hauptmenüs zuzugreifen, wählen Sie die Auswahloptionen in der Taskleiste auf der linken Seite der Systemseite aus.

Das Tivoli Identity Manager-System besteht aus mindestens einer Organisation mit Tochtergesellschaftsentitäten wie beispielsweise Organisationseinheiten, Standorte und Geschäftspartnerorganisationen, die sich in abhängigen Beziehungen zu über- und untergeordneten Entitäten befinden. Jede Tivoli Identity Manager-Entität kann Personen enthalten, die Sie bestimmten ITIM-Gruppen und Organisationsberechtigungsklassen zuordnen können. Die Berechtigungsklasse des Systemadministrators kann Personen zugeordnet werden, die uneingeschränkten Zugriff auf alle Funktionsbereiche in Tivoli Identity Manager benötigen.

Organisationsverwaltung

Die Verwaltung einer Organisation erfolgt über die Registerkarte ″Eigene Organisation″ in der Navigationsleiste des Hauptmenüs. Durch Klicken auf **Eigene Organisation** wird die Taskleiste ″Organisation″ im linken Bereich der Seite angezeigt. Die Taskleiste enthält Funktionen, die Sie in den Organisationen und ihren jeweiligen Tochtergesellschaftsentitäten sowie für die Personen in diesen Organisationen und sonstigen Entitäten ausführen können.

Wenn Sie auf **Eigene Organisation** klicken, zeigt Tivoli Identity Manager eine aus zwei Teilfenstern zusammengesetzte Seite an. Im linken Teilfenster wird eine Liste der Organisationen in einem Format angezeigt, das zum Anzeigen von Tochtergesellschaftsentitäten eingeblendet bzw. ausgeblendet werden kann. Diese Liste wird zum Auswählen einer Entität verwendet. Das rechte Teilfenster zeigt eine Auflistung von Entitäten (Organisationen, Standorten, Organisationseinheiten, Geschäftspartnerorganisationen) oder Personen (der ausgewählten Entität) an.

Alle Tochtergesellschaftsentitäten können Tochtergesellschaften einer Organisation oder einer beliebigen anderen Entität sein. Es gelten keine Einschränkungen für die Hierarchie von Tochtergesellschaftsentitäten. Daher können beispielsweise Standorte andere Standorte und Organisationseinheiten andere Organisationseinheiten sowie beliebige andere Tochtergesellschaftsentitäten enthalten. An der Spitze der Organisationshierarchie muss jedoch immer eine Organisation stehen.

Personalverwaltung

Wenn Personen hinzugefügt werden, müssen diese entweder einer Organisation oder einem anderen Container wie beispielsweise einer Organisationseinheit, einer Geschäftspartnerorganisation, einer Verwaltungsdomäne oder einem Standort zugeordnet werden. Nachdem eine Person zu einer Organisation oder einem anderen Container hinzugefügt wurde, können für die betreffende Person Services eingerichtet werden, mit deren Hilfe die Person auf eine verwaltete Ressource einschließlich Tivoli Identity Manager Server zugreifen kann.

Verwaltung von Services

Sie können einen Service zu einer Organisation hinzufügen und Personen dadurch die Möglichkeit eröffnen, auf diesen Service zuzugreifen. Ein Service ist eine verwaltete Ressource wie beispielsweise Windows NT® Server, MS Exchange Server oder sogar Tivoli Identity Manager Server. Der Vorgang, den Zugriff auf eine verwaltete Ressource zu ermöglichen, wird als *Einrichtung* bezeichnet. Da Tivoli Identity Manager Server auch zu den Services gehört, die verwaltet werden können, muss dieser Service für bestimmte Personen eingerichtet werden, selbst wenn dies möglicherweise nur dazu erforderlich ist, um auf die eigenen Tivoli Identity Manager-Accounts und persönlichen Informationen zuzugreifen und diese zu verwalten. Wurde kein ITIM-Service für eine Person eingerichtet, hat die betreffende Person keinen Zugriff auf ihre eigenen Informationen in Tivoli Identity Manager. Wurden jedoch Services für eine Person eingerichtet, hat diese Person auch Zugriff auf die betreffenden Services.

Einrichtung

Die Einrichtung von Services erfolgt nicht für einzelne Personen, sondern lediglich für Organisationsberechtigungsklassen. Benötigt eine Person Zugriff auf einen bestimmten Service, muss diese Person einer Organisationsberechtigungsklasse zugeordnet werden, für die dieser Service eingerichtet wurde.

Personen können nur dann als Benutzer von Tivoli Identity Manager agieren, wenn sie einer ITIM-Gruppe zugeordnet wurden. ITIM-Gruppen verfügen über verschiedene Zugriffstypen, die durch ACI-Routinen gesteuert werden. Eine ACI-Routine definiert drei Faktoren:

- Die Funktionstypen, für die der ITIM-Gruppe die Zugriffsrechte erteilt werden.
- Die Typen von Organisations- oder Tochtergesellschaftsentitäten, für die die erteilten Funktionen ausgeführt werden dürfen.
- Die Ebene innerhalb der Organisationshierarchie, auf der die erteilten Funktionen ausgeführt werden dürfen.

Kapitel 2. Anmeldung

Die Anmelderoutine verhindert, dass Benutzer ohne entsprechende Berechtigung auf das Tivoli Identity Manager-System zugreifen, während sie Ihnen ermöglicht, auf die Bereiche zuzugreifen, für die Sie eine Zugriffsberechtigung besitzen, und in dem Fall, dass Sie Ihr Kennwort vergessen haben, eine Prozedur für vergessene Kennwörter bereitstellt.

Um sich bei Tivoli Identity Manager anzumelden, müssen Sie Ihre Benutzer-ID und Ihr Kennwort eingeben. Ihr Account verfügt über die erforderlichen Berechtigungen zum Ausführen Ihrer Aufgaben. Ihr Kennwort muss mit den in Ihrer Organisation geltenden Kennwortregeln konform sein.

Um sich bei Tivoli Identity Manager anzumelden, gehen Sie wie folgt vor:

1. Geben Sie Ihre Benutzer-ID ein, und drücken Sie auf die Tabulatortaste, um zum Feld **Kennwort** zu gelangen.
2. Geben Sie Ihr Kennwort ein, und drücken Sie entweder die **Eingabetaste** oder klicken Sie auf **Anmelden**.

Auswahl der Sprache

Tivoli Identity Manager ermöglicht den Benutzern, die Sprache auszuwählen, die im Tivoli Identity Manager-System verwendet werden soll.

Um die Sprache zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der unteren linken Ecke der Seite "Anmeldung" auf die Option **Andere Sprache auswählen**.

   Die Seite "Auswahl der Sprache" wird geöffnet.
2. Klicken Sie auf die gewünschte Sprache.

   Tivoli Identity Manager Server wird jetzt für die Verwendung der ausgewählten Sprache konfiguriert. Die Seite "Anmeldung" wird erneut angezeigt.
3. Melden Sie sich beim System an, und führen Sie die gewünschten Aktivitäten aus.

Wenn Sie sich mit der Funktion für einmalige Anmeldung anmelden und eine Sprache auswählen wollen, fügen Sie der Websiteadresse `/language` hinzu. Geben Sie zum Beispiel Folgendes ein:

`https://`*`eigener_standort.eigenes_unternehmen`*`.com/itim/enrole/language`

Weitere Informationen zur Konfiguration der Standardsprache für Ihren Webbrowser finden Sie im Handbuch *Tivoli Identity Manager Server Configuration Guide*.

Abrufen neuer Kennwörter

Nach der Einrichtung eines neuen Accounts für eine Person benachrichtigt das System diese Person per E-Mail, wobei die im Datensatz für persönliche Informationen angegebene E-Mail-Adresse verwendet wird. Das System kann so konfiguriert werden, dass die Person eine E-Mail-Nachricht mit dem Accountkennwort in Klartext oder einer URL- und Transaktions-ID-Nummer erhält.

Die folgenden Prozeduren erläutern, wie ein neues Kennwort unter Verwendung der URL und der Transaktions-ID abgerufen wird. Der Benutzer muss in der Lage sein, den geheimen Schlüssel (Shared Secret) anzugeben, um das neue Kennwort abrufen zu können.

Um ein neues Kennwort abzurufen, gehen Sie wie folgt vor:

1. Klicken Sie auf die URL in der E-Mail, um die Seite "Kennwort abrufen" anzuzeigen.

   Die Seite "Kennwort abrufen" wird geöffnet. Das Feld **Transaktions-ID** enthält bereits die Transaktions-ID-Nummer, die in der E-Mail-Nachricht enthalten war.
2. Geben Sie den geheimen Schlüssel in das Textfeld **Shared Secret** ein, und klicken Sie auf **Übergeben**.

   Die Seite "Abrufen des Kennworts" wird geöffnet.
3. Notieren Sie sich das Kennwort, und klicken Sie auf **Fertig**.

   Die Seite "Abrufen des Kennworts" wird geschlossen.

   Wichtig: Notieren Sie unbedingt das Kennwort, da diese Seite nicht erneut geöffnet werden kann.

Kennwort vergessen (Kennwortprüffrage des Challenge/Response-Verfahrens)

Vergisst ein Benutzer sein Kennwort, kann er sich dennoch beim System anmelden, wenn er die Kennwortprüffragen des Challenge/Response-Verfahrens korrekt beantwortet. Nachdem der Benutzer die Prüffragen beantwortet hat, reagiert Tivoli Identity Manager auf eine der folgenden Arten und Weisen, wobei das Reaktionsverhalten von der Konfiguration des Systems abhängt:

- Der Benutzer wird beim System angemeldet und dazu gezwungen, sein Kennwort unverzüglich zu ändern.
- Dem Benutzer wird ein neues Kennwort per E-Mail in Textform zugesendet.
- Dem Benutzer wird per E-Mail eine Verknüpfung zugesendet, über die er sein neues Kennwort unter Angabe des geheimen Schlüssels (Shared Secret) abrufen kann.

Um sich über das Challenge/Response-Verfahren anzumelden, gehen Sie wie folgt vor:

1. Geben Sie im Feld **Benutzer-ID** Ihren Anmeldenamen ein.
2. Klicken Sie auf die Verknüpfung **Kennwort vergessen?** auf der Anmeldeseite.

   Anmerkung: Ist das Challenge/Response-Verfahren für Kennwörter nicht aktiviert, wird die folgende Nachricht angezeigt:

   ```
   Das Challenge/Response-Verfahren für Kennwörter ist gegenwärtig
   inaktiviert.

   Bitte  nehmen Sie Kontakt mit Ihrem Identity Manager-System-
   administrator auf, um nähere Informationen zu erhalten.
   ```
3. Beantworten Sie die Kennwortprüffragen des Challenge/Response-Verfahrens, und klicken Sie auf **Übergeben**.

   Das System reagiert je nach Konfiguration auf eine der nachstehend beschriebenen Arten und Weisen:

   - Der Benutzer wird beim System angemeldet und dazu gezwungen, sein Kennwort unverzüglich zu ändern.

- Dem Benutzer wird ein neues Kennwort per E-Mail in Textform zugesendet.
- Dem Benutzer wird per E-Mail eine Verknüpfung zugesendet, über die er sein neues Kennwort unter Angabe des geheimen Schlüssels (Shared Secret) abrufen kann.

Konfiguration des erzwungenen Challenge/Response-Verfahrens

Wenn das Challenge/Response-Verfahren für Kennwörter aktiviert ist, kann ein Benutzer auch dann auf das Tivoli Identity Manager-System zugreifen, wenn er sein Kennwort vergessen hat. Ist das Challenge/Response-Verfahren für Kennwörter nicht aktiviert, muss der Benutzer den Systemadministrator kontaktieren, um Zugriff auf das Tivoli Identity Manager-System zu erhalten.

Nach jeder erstmaligen Aktivierung oder nachfolgenden Änderung des Challenge/Response-Verfahrens für Kennwörter müssen die Benutzer ihre Antworten auf die Kennwortprüffragen des Challenge/Response-Verfahrens festlegen. Abhängig von dem jeweiligen Challenge/Response-Modus für Kennwortprüffragen muss ein Benutzer gegebenenfalls Prüffragen definieren und Antworten auf die Prüffragen angeben oder aber Prüffragen auswählen und Antworten auf die ausgewählten Prüffragen angeben oder auch Antworten auf die angezeigten Prüffragen angeben.

Folgen Sie den Aufforderungen am Anfang jeder Seite, um die Funktionen des Challenge/Response-Verfahrens zu konfigurieren.

Abrufen eines Kennworts

Wurde Tivoli Identity Manager Server dazu konfiguriert, dem Benutzer eine E-Mail-Nachricht mit einer Verknüpfung zum Abrufen des neuen Kennworts zuzusenden, muss der Benutzer in der Lage sein, den geheimen Schlüssel (Shared Secret) anzugeben, um das neue Kennwort abrufen zu können.

Um ein Kennwort abzurufen, gehen Sie wie folgt vor:

1. Klicken Sie auf die URL in der E-Mail, um die Seite "Kennwort abrufen" anzuzeigen.

   Die Seite "Kennwort abrufen" wird geöffnet. Das Feld **Transaktions-ID** enthält bereits die Transaktions-ID-Nummer, die in der E-Mail-Nachricht enthalten war.
2. Geben Sie den geheimen Schlüssel in das Textfeld **Shared Secret** ein, und klicken Sie auf **Übergeben**.

   Die Seite "Abrufen des Kennworts" wird geöffnet.
3. Notieren Sie sich das Kennwort, und klicken Sie auf **Fertig**.

   Die Seite "Abrufen des Kennworts" wird geschlossen.

   Wichtig: Notieren Sie unbedingt das Kennwort, da diese Seite nicht erneut geöffnet werden kann.

Wichtig: Sie **müssen** sich unmittelbar nach dem Abrufen des neuen Kennworts anmelden und Ihr Kennwort ändern. Die Transaktions-ID verliert ihre Gültigkeit, nachdem Sie auf **Fertig** geklickt haben, und Sie können dementsprechend das neue Kennwort **nicht** erneut abrufen.

Erzwungene Änderung des Kennworts

Benutzer können dazu gezwungen werden, ihr Kennwort bei der ersten Anmeldung mit einem neuen Account beim Tivoli Identity Manager Server-System oder bei der nächsten Anmeldung mit einem bestehenden Account zu ändern.

Anmerkung: Diese Funktion gilt nur für Tivoli Identity Manager-Accounts.

Benutzer, die dazu gezwungen werden, ihr Kennwort zu ändern, werden unmittelbar nach der Anmeldung automatisch zur Seite `Erzwungene Änderung des Kennworts > Kennwort ändern` umgeleitet. Der Benutzer hat erst dann Zugriff auf die Funktionen im Tivoli Identity Manager-System, nachdem er sein Kennwort geändert hat.

Ablauf von Kennwörtern

Administratoren haben die Möglichkeit, die Laufzeit von Benutzerkennwörtern durch Angabe eines entsprechenden Wertes zu begrenzen. Diese Einstellung erfolgt unter:

`Konfiguration > Merkmale > Ablaufzeitraum des Kennworts`

Benutzer, die dazu gezwungen werden, ihr Kennwort nach dessen Ablauf zu ändern, werden unmittelbar nach der Anmeldung automatisch zur Seite `Erzwungene Änderung des Kennworts > Kennwort ändern` umgeleitet. Der Benutzer hat erst dann Zugriff auf die Funktionen im Tivoli Identity Manager-System, nachdem er sein Kennwort geändert hat.

Kapitel 3. Einheitliche Funktionen

Im Tivoli Identity Manager-System werden einige einheitliche Funktionen verwendet. Hierzu gehören die Navigationsfunktionen (Navigationsleiste im Hauptmenü und Taskleiste) und das Gültigkeitsdatum.

Navigation

Für die Navigation im Tivoli Identity Manager-System werden folgende Hauptfunktionen verwendet:

- Die Navigationsleiste des Hauptmenüs
- Die Taskleiste
- Die Organisationsbaumstruktur

Weitere Informationen zu den jeweiligen Navigationsfunktionen enthalten die nachfolgenden Abschnitte.

Navigationsleiste des Hauptmenüs

Die Navigationsleiste des Hauptmenüs befindet sich am Anfang jeder Seite und enthält folgende Optionen:

- Ausgangsposition
- Bericht
- Hilfe

Anhand dieser Optionen kann der Benutzer zügig zu bestimmten Bereichen im Tivoli Identity Manager-System navigieren.

Anmerkung: Die aktuelle Position (Standort) innerhalb des Systems wird auf jeder Seite im Navigationspfad angezeigt. Dem Navigationspfad ist jeweils der Ausdruck `Aktuelle Position:` vorangestellt.

Taskleiste

Die Taskleiste befindet sich am linken Rand jeder Seite der Systembereiche **Ausgangsposition**, **Eigene Organisation**, **Einrichtung** sowie **Bericht** und zeigt zusätzliche Unterbereiche zu jedem Stichwortbereich der Navigationsleiste des Hauptmenüs an.

Die folgende Tabelle zeigt, welche Taskleistenoptionen für das jeweilige Stichwort in der Navigationsleiste des Hauptmenüs verfügbar sind.

Stichwort in der Navigationsleiste des Hauptmenüs	Optionen in der Taskleiste
Ausgangsposition	Kennwörter verwalten Accounts verwalten Auf To-do-Liste zugreifen Anstehende Anforderungen anzeigen Beendete Anforderungen anzeigen Auf persönliche Informationen zugreifen Berechtigung delegieren Challenge/Response-Verfahren für Kennwörter
Bericht	Bericht ausführen Zugriff steuern Schema entwerfen Bericht entwerfen Daten synchronisieren
Hilfe	*Keine Optionen in der Taskleiste verfügbar*

Gültigkeitsdatum

Das Gültigkeitsdatum ist der geplante Zeitpunkt (Datum und Uhrzeit), an dem ein Ereignis eintritt. Sie können das genaue Datum und die genaue Uhrzeit für das Ereignis auswählen oder aber das Markierungsfeld für die sofortige Planung der Ausführung auswählen, damit das Ereignis sofort eingeleitet wird.

Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Übergeben**, damit die Verarbeitung erfolgt. Anschließend wird die Seite mit der Liste der geänderten Entitäten erneut angezeigt. Gegebenenfalls müssen Sie auf **Aktualisieren** klicken, damit der Inhalt der angezeigten Seiten aktualisiert wird.

Hilfe

Über das Thema ″Hilfe″ in der Navigationsleiste des Hauptmenüs wird die Onlinehilfe für Tivoli Identity Manager Server in einem separaten Fenster geöffnet. Die Onlinehilfe enthält Informationen über Konzepte und Funktionen im Tivoli Identity Manager-System.

Darüber hinaus enthält jede Seite auch eine kontextabhängige Verknüpfung zur Onlinehilfe. Diese Verknüpfung wird durch die mit einem Fragezeichen versehene Schaltfläche in der oberen rechten Ecke jeder Seite aufgerufen.

Kapitel 4. Ausgangsposition

An der **Ausgangsposition** können Benutzer Informationen anzeigen und bearbeiten, die sie selbst direkt betreffen. Jede Person, die über die Berechtigung zum Zugreifen auf die eigenen Informationen verfügt, kann an der Ausgangsposition die eigenen persönlichen Informationen bearbeiten und die eigenen Aktionselemente anzeigen.

Die **Ausgangsposition** ermöglicht den Benutzern die Durchführung der folgenden Aktionen:

- Kennwörter für ihre eigenen Accounts verwalten
- Ihre eigenen Accounts verwalten
- Auf die eigene To-do-Liste zugreifen
- Die eigenen anstehenden und beendeten Anforderungen anzeigen
- Auf die eigenen persönlichen Informationen zugreifen
- Berechtigungen an andere Benutzer übertragen
- Die Antworten auf die Kennwortprüffragen des Challenge/Response-Verfahrens festlegen

Weitere Informationen zu den jeweiligen Taskleistenoptionen finden Sie in den entsprechenden Abschnitten.

Kennwortverwaltung

Der Zugriff auf den Bereich **Kennwortverwaltung** unter der **Ausgangsposition** erfolgt über die Option **Kennwörter verwalten** der Taskleiste **Ausgangsposition**. In diesem Bereich können Benutzer alle Kennwörter für alle ihre Accounts zentral von einem Ort aus verwalten.

Die Seite ″Kennwortverwaltung″ beinhaltet die folgenden Felder und Funktionen:

Feldname	Feldtyp	Beschreibung
Neues Kennwort	Textfeld	Textfeld zum Eingeben des neuen Kennworts.
Kennwort bestätigen	Textfeld	Textfeld zum Bestätigen des Kennworts durch erneute Eingabe
Kennwort erstellen	Markierungsfeld	Mit diesem Markierungsfeld wird festgelegt, ob das System ein neues Kennwort für den Account generieren soll. Wird dieses Markierungsfeld ausgewählt, generiert das System ein neues Kennwort für den Account und sendet die Informationen, die zum Abrufen des neuen Kennworts erforderlich sind, per E-Mail an die E-Mail-Adresse, die dem Account zugeordnet ist.

Feldname	Feldtyp	Beschreibung
Gültigkeitsdatum (Auswahlfeld)	Markierungsfeld (Für sofortige Ausführung planen) in Dropdown-Menüs	Auswahlfelder, mit denen der Zeitpunkt (Uhrzeit und Datum) festgelegt wird, ab dem das neue Kennwort in Kraft tritt. Weitere Informationen hierzu finden Sie unter „Gültigkeitsdatum" auf Seite 10.
Service (Tabelle)	Text	Tabelle mit einer Auflistung der Services, für die der Benutzer Accounts besitzt. Die Tabelle enthält fünf Spalten. Weitere Informationen zur Tabelle **Service** enthält die nachstehende Tabelle.
Übergeben	Schaltfläche	Mit dieser Schaltfläche werden die Änderungen an das System übergeben.
Zurücksetzen	Schaltfläche	Mit dieser Schaltfläche werden die Werte auf der Seite auf die zuletzt im System gespeicherten Werte zurückgesetzt.
Kombinierte Kennwortregeln anzeigen	Hyperlink	Dieser Hyperlink öffnet eine Seite, die eine Kombination der Kennwortregeln für alle aufgeführten Services anzeigt.

Die Tabelle **Services** enthält eine Auflistung der Services, für die der Benutzer Accounts besitzt. Die folgende Tabelle erläutert jede Spalte der Tabelle **Services**.

Spaltenname	Beschreibung
(Markierungsfeld)	Bei Auswahl des Markierungsfeldes werden die durchgeführten Änderungen auf den Account für den entsprechenden Service angewendet.
Regeln	Diese Spalte enthält Symbole, die eine Verbindung zu den Kennwortregeln für einen bestimmten Service herstellen.
Service	Der Name des Services.
Anmeldename	Die Anmelde-ID des Benutzers für den entsprechenden Service.
Status	Der Status des Benutzeraccounts.

Um Ihr Kennwort zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Kennwörter verwalten**.

   Die Seite "Kennwort verwalten" wird geöffnet.
3. Geben Sie im Textfeld **Neues Kennwort** ein neues Kennwort ein und bestätigen Sie es im Feld **Kennwort bestätigen** durch die erneute Eingabe **ODER** wählen Sie das Markierungsfeld **Kennwort erstellen** aus.

   Bei Auswahl des Markierungsfelds **Kennwort erstellen** generiert Tivoli Identity Manager ein Kennwort für den Benutzer und sendet dieses an die E-Mail-Adresse, die dem Account zugeordnet ist.

4. Wählen Sie ein Gültigkeitsdatum und eine Uhrzeit aus **ODER** wählen Sie das Markierungsfeld **Für sofortige Ausführung planen** aus.
5. Wählen Sie die Markierungsfelder neben den Namen der Services aus, deren Kennwörter geändert werden sollen.
6. Prüfen Sie, ob das Kennwort den Kennwortregeln für die ausgewählten Services entspricht. Klicken Sie dazu auf das Symbol **Anzeigen** neben den Services.

   Wenn ein Benutzer die Kennwörter für mehrere Services ändern möchte, kann hierzu auf die Verknüpfung **Kombinierte Kennwortregeln anzeigen** geklickt werden. Damit werden die einschränkenden Komponenten für jede Gruppe von Kennwortregeln angezeigt.
7. Klicken Sie auf **Übergeben**.

   Die Änderungen werden übergeben und treten zum geplanten Zeitpunkt in Kraft.

Accountverwaltung

Der Zugriff auf den Bereich **Accountverwaltung** unter der **Ausgangsposition** erfolgt über die Option **Accounts verwalten** der Taskleiste **Ausgangsposition**. In diesem Bereich können Benutzer alle eigenen Accounts zentral von einem Ort aus verwalten.

Die Seite ″Accountverwaltung″ ist wie folgt aufgebaut:

Spaltenname	Beschreibung
Markierungsfeld	Dient zum Auswählen des in der Zeile aufgeführten Accounts.
Konformitätsstatus	Gibt an, ob ein Account mit den aktuellen Richtlinien konform ist. Die nachstehende Tabelle enthält die Konformitätsmarkierungen und zugehörigen Beschreibungen.
Benutzer-ID	Die Benutzer-ID für jeden Account.
Servicename	Der Service, für den der Account verwendet wird.
Status	Der Status des Accounts.

Der Konformitätsstatus wird durch eine Markierung angezeigt. Insgesamt stehen vier verschiedene Markierungen zur Verfügung. Jede Markierung verfügt über eine eigene Definition. Die folgende Tabelle erläutert die jeweilige Bedeutung der Konformitätsmarkierungen.

Markierung für den Konformitätsstatus	Beschreibung
	Eine leere Grafik kennzeichnet Accounts, die mit den vorhandenen Einrichtungsrichtlinien konform sind. Diese Grafik kann so geändert werden, dass ein Häkchen oder ein grünes Licht angezeigt wird. Der Name der entsprechenden Grafikdatei lautet `acct_compliant.gif`.

Markierung für den Konformitätsstatus	Beschreibung
	Ein Fragezeichen wird nur für Accounts verwendet, die von einem Datenabgleich zurückgegeben wurden. Diese Markierung gibt an, dass während der Durchführung des Datenabgleichs keine Richtlinienprüfung durchgeführt wurde. Alle Accounts, die vom Datenabgleich zurückgegeben wurden, sind mit dieser Markierung versehen.
	Das Warnsymbol gibt an, dass ein Account für den Benutzer vorhanden sein darf, jedoch mindestens eines der Accountattribute nicht mit den vorhandenen Richtlinien konform ist.
	Das Symbol für die Nichtkonformität gibt eines von zwei Szenarien an: • Der Benutzer darf keinen Zugriff auf die angegebene Ressource erhalten, und der Account darf eigentlich nicht vorhanden sein. • Für die Ressource ist keine Einrichtungsrichtlinie definiert.

Die Accounts können nach Benutzer-ID, Konformität oder Status sortiert werden.

Ausführliche Informationen zu einem Account werden angezeigt, wenn auf die Benutzer-ID des Accounts geklickt wird. Alle an einem Account vorgenommenen Änderungen können für sofortige Wirksamkeit (Für sofortige Ausführung planen) oder für einen späteren Zeitpunkt geplant werden.

Auf der Seite "Accountverwaltung" können Benutzer anhand der bereitgestellten Optionen die folgenden Aktionen durchführen:

- Neue Accounts für vorhandene Services hinzufügen
- Vorhandene Accounts ändern
- Accounts aussetzen (inaktivieren)
- Einrichtung von Accounts zurücknehmen (Accounts löschen)
- Accounts wiederherstellen (erneut aktivieren)
- Kennwörter ändern

Hinzufügen neuer Accounts

Benutzer mit entsprechender Berechtigung können für sich selbst neue Accounts zu vorhandenen Services hinzufügen.

Um einen neuen Account hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Accounts verwalten**.
   Die Seite "Accountverwaltung" wird geöffnet.
3. Klicken Sie auf **Neu**.
   Die Seite "Service einrichten" wird geöffnet.
4. Wählen Sie den Radioknopf für den Service aus, für den Sie einen neuen Account hinzufügen wollen, und klicken Sie auf **Weiter**.
   Die Seite "Neuen Service einrichten" wird geöffnet. Die auf dieser Seite enthaltenen Felder hängen von dem jeweils ausgewählten Servicetyp ab.
5. Geben Sie in der Anzeige die zutreffenden Daten ein.

Anmerkung: Wenn das Markierungsfeld **Kennwort bei der nächsten Anmeldung ändern?** ausgewählt ist, muss der Benutzer das Kennwort ändern, wenn er sich erstmals beim System anmeldet.

6. Klicken Sie auf **Übergeben**.

   Die Seite "Kennwort eingeben und Gültigkeitsdatum | Uhrzeit auswählen" wird geöffnet.
7. Geben Sie ein Kennwort für den Account ein, und bestätigen Sie das Kennwort durch erneute Eingabe im Textfeld **Kennwort bestätigen**.

   Achten Sie darauf, dass das Kennwort mit den geltenden Kennwortregeln konform ist, da es ansonsten zurückgewiesen wird.
8. Wählen Sie Gültigkeitsdatum und Uhrzeit aus, und klicken Sie auf **Übergeben**.

   Weitere Informationen hierzu finden Sie unter „Gültigkeitsdatum" auf Seite 10.

   Die Anforderung wird übergeben, und die Seite "Accountverwaltung" wird erneut angezeigt.
9. Klicken Sie auf **Aktualisieren**, um den Inhalt der Tabelle auf den neuesten Stand zu bringen.

Ändern vorhandener Accounts

Benutzer mit entsprechender Berechtigung können auf der Seite "Accountverwaltung" einen ihrer vorhandenen Accounts ändern.

Um einen vorhandenen Account zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Accounts verwalten**.

   Die Seite "Accountverwaltung" wird geöffnet.
3. Klicken Sie auf den Namen des Accounts, den Sie ändern wollen.

   Die Seite "Account ändern" wird geöffnet.
4. Ändern Sie die Accountinformationen wie gewünscht, und klicken Sie anschließend auf **Übergeben**.

   Anmerkung: Die Benutzer-ID ist ein Musseingabefeld und erfordert eine Eingabe, damit der Vorgang fortgesetzt werden kann.
   Wenn das Markierungsfeld **Kennwort bei der nächsten Anmeldung ändern?** ausgewählt ist, muss der Benutzer das Kennwort ändern, wenn er sich erstmals beim System anmeldet.

   Die Seite "Kennwort eingeben und Gültigkeitsdatum | Uhrzeit auswählen" wird geöffnet.
5. Wählen Sie Gültigkeitsdatum und Uhrzeit für das Inkrafttreten der Änderungen aus oder wählen Sie das Markierungsfeld **Für sofortige Ausführung planen** aus.

   Weitere Informationen hierzu finden Sie unter „Gültigkeitsdatum" auf Seite 10.
6. Klicken Sie auf **Übergeben**.

   Die Anforderung wird übergeben, und die Seite "Accountverwaltung" wird erneut angezeigt.

   Informationen dazu, wie ein Account wiederhergestellt wird, finden Sie unter „Wiederherstellen von Accounts" auf Seite 16.
7. Klicken Sie auf **Aktualisieren**, um den Inhalt der Tabelle auf den neuesten Stand zu bringen.

Aussetzen von Accounts oder Zurücknehmen der Einrichtung von Accounts

Benutzer mit entsprechender Berechtigung können auf der Seite "Accountverwaltung" ihre eigenen Accounts aussetzen oder die Einrichtung ihrer eigenen Accounts zurücknehmen. Das Aussetzen eines Accounts bewirkt die Inaktivierung des Accounts, sodass sich der Accounteigner nicht mehr beim Tivoli Identity Manager-System anmelden kann. Der Account selbst wird jedoch nicht aus dem System gelöscht. Durch die Zurücknahme der Einrichtung eines Accounts wird der entsprechende Account aus dem Tivoli Identity Manager-System gelöscht.

Um einen Account auszusetzen oder die Einrichtung eines Accounts zurückzunehmen, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Accounts verwalten**.

   Die Seite "Accountverwaltung" wird geöffnet.
3. Wählen Sie das Markierungsfeld neben jedem Account aus, dessen Einrichtung zurückgenommen oder der ausgesetzt werden soll.
4. Klicken Sie auf **Einrichtung zurücknehmen** bzw. auf **Aussetzen**.

   Je nach ausgewählter Option wird die Seite "Einrichtung von Service(s) zurücknehmen" oder die Seite "Service(s) aussetzen" geöffnet.
5. Wählen Sie Gültigkeitsdatum und Uhrzeit aus oder wählen Sie das Markierungsfeld **Für sofortige Ausführung planen** aus.

   Weitere Informationen hierzu finden Sie unter „Gültigkeitsdatum" auf Seite 10.
6. Klicken Sie auf **Übergeben**.

   Die Anforderung wird übergeben, und die Seite "Accountverwaltung" wird erneut angezeigt.

   Informationen dazu, wie ein Account wiederhergestellt wird, finden Sie unter „Wiederherstellen von Accounts" auf Seite 16.

Wiederherstellen von Accounts

Benutzer mit entsprechender Berechtigung können auf der Seite "Accountverwaltung" ihre eigenen ausgesetzten Accounts wiederherstellen (reaktivieren). Bei der Wiederherstellung von Accounts ist es erforderlich, ein neues Kennwort einzugeben oder zu erstellen.

Um einen Account wiederherzustellen, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Accounts verwalten**.

   Die Seite "Accountverwaltung" wird geöffnet.
3. Wählen Sie jeweils das Markierungsfeld neben den Namen der Accounts aus, die wiederhergestellt werden sollen, und klicken Sie anschließend auf **Wiederherstellen**.

   Nur ausgesetzte Accounts können wiederhergestellt werden.
4. Geben Sie ein **Neues Kennwort** ein und bestätigen Sie dieses. Wahlweise können Sie auch das Markierungsfeld **Kennwort erstellen** auswählen.

   Bei Auswahl des Markierungsfelds **Kennwort erstellen** generiert Tivoli Identity Manager ein Kennwort und sendet dieses an die E-Mail-Adresse, die dem Account zugeordnet ist.
5. Wählen Sie Gültigkeitsdatum und Uhrzeit aus oder wählen Sie das Markierungsfeld **Für sofortige Ausführung planen** aus.

6. Klicken Sie auf **Übergeben**.
   Die Anforderung wird übergeben, und die Seite ″Accountverwaltung″ wird erneut angezeigt.
7. Klicken Sie auf **Aktualisieren**, um den Inhalt der Tabelle auf den neuesten Stand zu bringen.

Ändern von Kennwörtern

ITIM-Benutzer können die Kennwörter für ihre Accounts auf der Seite ″Accountverwaltung″ oder auf der Seite ″Kennwort verwalten″ ändern.

Die Möglichkeit, alle Accounts von einer zentralen Position aus verwalten zu können, versetzt die Benutzer in die Lage, Kennwörter für mehrere Accounts gleichzeitig festzulegen. Wenn das neue Kennwort jedoch nicht den Kennwortregeln für die jeweiligen Services entspricht, schlägt die Anforderung fehl und das Kennwort wird nicht geändert. Benutzer sollten prüfen, ob die Anforderung erfolgreich durchgeführt und beendet wurde, bevor sie versuchen, sich mit dem neuen Kennwort bei der gewünschten Ressource anzumelden. Die Ergebnisse der Anforderungen können auf der Seite ″Beendete Anforderungen″ eingesehen werden. (Weitere Informationen hierzu finden Sie unter „Beendete Anforderungen” auf Seite 20.)

Die Änderung von Kennwörtern auf der Seite ″Accountverwaltung″ ähnelt dem Vorgang zum Ändern von Kennwörtern auf der Seite ″Kennwörter verwalten″. (Weitere Informationen zur Seite ″Kennwörter verwalten″ finden Sie unter „Kennwortverwaltung” auf Seite 11.)

Um das Kennwort für einen Account zu ändern, gehen Sie wie folgt vor:
1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Accounts verwalten**.
   Die Seite ″Accountverwaltung″ wird geöffnet.
3. Wählen Sie jeweils das Markierungsfeld neben den Namen der Accounts aus, deren Kennwörter geändert werden sollen, und klicken Sie anschließend auf **Kennwort ändern**.
   Die Seite ″Kennwort ändern″ der Accountverwaltung wird geöffnet.
4. Geben Sie im Textfeld **Neues Kennwort** ein neues Kennwort ein und bestätigen Sie dieses durch erneute Eingabe im Feld **Kennwort bestätigen**, **ODER** wählen Sie das Markierungsfeld **Kennwort erstellen** aus. Bei Auswahl des Markierungsfelds **Kennwort erstellen** generiert Tivoli Identity Manager ein Kennwort und sendet dieses an die E-Mail-Adresse, die dem Account zugeordnet ist.
5. Wählen Sie Gültigkeitsdatum und Uhrzeit aus **ODER** wählen Sie das Markierungsfeld **Für sofortige Ausführung planen** aus. Weitere Informationen hierzu finden Sie unter „Gültigkeitsdatum” auf Seite 10.
6. Prüfen Sie, ob jeweils das Markierungsfeld neben den Namen der Accounts, deren Kennwörter geändert werden sollen, ausgewählt ist.
7. Prüfen Sie, ob das Kennwort jeweils den Kennwortregeln für die ausgewählten Services entspricht. Klicken Sie hierzu auf das Symbol **Anzeigen** neben den betreffenden Services. Wenn Sie die Kennwörter für mehrere Services ändern, klicken Sie auf die Verknüpfung **Kombinierte Kennwortregeln anzeigen**, damit eine kombinierte Auflistung der einschränkenden Komponenten für jede Gruppe von Kennwortregeln angezeigt wird.
8. Klicken Sie auf **Übergeben**.
   Die Anforderung wird übergeben, und die Seite ″Accountverwaltung″ wird erneut angezeigt.

To Do-Liste

Auf der Seite ″To-do-Liste″ können ITIM-Benutzer Aktionselemente anzeigen und Aktionselemente ausführen, die ihnen zugeordnet wurden. Diese Aktionselemente können Anforderungen für Genehmigungen oder Informationsanforderungen sein. Die in der To-do-Liste aufgeführten Aktionselemente sind Bestandteil von Arbeitsablaufprozessen, die nur mit einer Antwort vom ITIM-Benutzer korrekt ausgeführt werden können.

Auf der Seite ″To-do-Liste″ können Benutzer Informationen zu einer Anforderung liefern und Anforderungen genehmigen, zurückweisen oder annullieren. Es besteht auch die Möglichkeit, die Anzeige der Seite ″To-do-Liste″ zu aktualisieren, um neu übergebene Aktionselemente zu erfassen und anzuzeigen. Anforderungen für Genehmigungen oder Informationen werden normalerweise von anderen Benutzern im System generiert.

Anmerkung: Anforderungen, die einer Genehmigung durch den Anforderer bedürfen, werden automatisch genehmigt. Ist mehr als eine Unterschriftsberechtigung erforderlich, wird nur diejenige Anforderung automatisch genehmigt, die an die eigene Warteschlange des Anforderers gesendet wurde. Die Anforderung muss die Genehmigung von zusätzlichen Unterschriftsberechtigten empfangen (wie vom Arbeitsablauf erfordert), damit die Anforderung vollständig verarbeitet und beendet werden kann.

Zu jedem Aktionselement werden die folgenden Informationen angezeigt:

Spaltenname	Beschreibung
Anforderungs-ID	Die der Anforderung zugeordnete Vorgangsnummer.
Aktion	Der Typ der vom Benutzer angeforderten Aktion.
Datum der Übergabe	Das Datum, an dem die Anforderung für eine Aktion übergeben wurde.
Anforderungsempfänger	Der Name des Benutzers, der die Aktion anfordert.
Betreff	Informationen zum Thema der Anforderung.
Status	Der aktueller Status der Anforderung.

Diese Seite kann anhand der Informationen in jeder Spalte sortiert werden.

Um ein Aktionselement vollständig auszuführen und zu beenden, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Auf To-do-Liste zugreifen**.
   Die Seite ″To-do-Liste″ wird geöffnet.
3. **OPTIONAL:** Ändern Sie die Sortierfolge der To-do-Liste. Klicken Sie dazu auf den Pfeil neben dem Namen des Felds, nach dem die Sortierung erfolgen soll, und wählen Sie das gewünschte Attribut aus.
4. **OPTIONAL:** Zeigen Sie die Anforderungen eines spezifischen Typs an, indem Sie im Dropdown-Menü **Typ** den entsprechenden Anforderungstyp auswählen.

5. **OPTIONAL:** Klicken Sie auf das Symbol **Details anzeigen** neben der Anforderungs-ID der entsprechenden Anforderung, um zusätzliche Informationen zu dem gewünschten Aktionselement anzuzeigen.

   Die Seite ″Anforderungsdetails″ wird geöffnet.
6. **OPTIONAL:** Klicken Sie auf **Abbrechen**, um zur Seite ″To-do-Liste″ zurückzukehren.
7. Klicken Sie in der Spalte ″Aktion″ auf die Verknüpfung des Elements, das durchgeführt und beendet werden soll.

   Die Seite ″Anforderung genehmigen/zurückweisen″ wird geöffnet, wenn es sich bei dem Aktionselement um eine Anforderung für Genehmigung/Zurückweisung handelt.
8. Führen Sie je nach Typ des durchzuführenden Aktionselements eine der folgenden Aktionen aus:
   - **Anforderung des Typs ″Genehmigen/Zurückweisen″**
     a. Wählen Sie den Radioknopf **Genehmigen** oder **Zurückweisen** aus.
     b. **Optional:** Geben Sie im Textfenster **Erklärung** eine kurze Erklärung für Ihre Entscheidung ein.
     c. **Optional:** Klicken Sie auf **Anforderungsdaten anzeigen**, um Informationen zur betreffenden Anforderung und die zugehörigen Einstellungen anzuzeigen.
     d. Klicken Sie auf **Übergeben**.

        Die Antwort wird übergeben, und die Seite ″To-do-Liste″ wird erneut angezeigt.
   - **Anforderungen des Typs ″Informationen zur Verfügung stellen″**
     a. Stellen Sie die angeforderten Informationen zur Verfügung.
     b. Klicken Sie auf **Übergeben**.

        Die Antwort wird übergeben, und die Seite ″To-do-Liste″ wird erneut angezeigt.

Anzeigen der Detailinformationen einer To-do-Liste

Benutzer können jederzeit die Detailinformationen zu den Anforderungen in ihrer To-do-Liste anzeigen.

Um Detailinformationen zu einer anstehenden Anforderung anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Auf To-do-Liste zugreifen**.

   Die Seite ″To-do-Liste″ wird geöffnet.
3. **OPTIONAL:** Ändern Sie die Sortierfolge der Anforderung. Klicken Sie dazu auf den Pfeil neben dem Namen des Felds, nach dem die Sortierung erfolgen soll, und wählen Sie das gewünschte Attribut aus.

   Die Anzeige der Seite ″To-do-Liste″ wird aktualisiert und enthält die Anforderungen jetzt in der Sortierung nach dem ausgewählten Attribut.
4. Klicken Sie auf das Symbol **Anzeigen** neben der Anforderung, deren Detailinformationen angezeigt werden sollen.

   Die Seite ″Anforderungsdetails″ wird geöffnet.
5. Wählen Sie die Registerkarte mit den Informationen aus, die Sie anzeigen wollen.
6. Klicken Sie auf jeder beliebigen Registerkarte auf **Abbrechen**, um zu der Seite ″To-do-Liste″ zurückzukehren.

Anstehende Anforderungen

Auf der Seite ″Anstehende Anforderungen″ können ITIM-Benutzer die Anforderungen anzeigen, die bereits an das Tivoli Identity Manager-System übergeben wurden, vom System jedoch noch nicht vollständig verarbeitet und beendet wurden. Wenn die Seite ″Anstehende Anforderungen″ angezeigt wird, sollte in regelmäßigen Zeitabständen auf **Aktualisieren** geklickt werden, um die Anzeige auf den neuesten Stand zu bringen, damit neu übergebene Anforderungen sowie vorhandene Anforderungen, die bereits beendet wurden, ebenfalls erfasst und angezeigt werden.

Anstehende Anforderungen können nach den folgenden Kriterien sortiert werden:

- Anforderungs-ID
- Datum der Übergabe
- Typ
- Anforderer
- Anforderungsempfänger
- Betreff
- Status

Beendete Anforderungen

Die Seite ″Beendete Anforderungen″ enthält eine Auflistung aller Anforderungen, die am betreffenden Tag abgeschlossen wurden. Der Benutzer kann die Sortierung der Informationen in den Spalten auf der Seite ändern, indem er auf die Pfeile am oberen Ende der jeweiligen Spalte klickt. Um Details zur jeweiligen Anforderung anzuzeigen, klicken Sie auf das Symbol **Anzeigen** neben der betreffenden Anforderungs-ID in der linken Hälfte der Seite.

Anmerkung: Um die von Tivoli Identity Manager angezeigten Informationen einzugrenzen, empfiehlt sich die Auswahl der Option **Anforderungen filtern**. Die Option **Anforderungen filtern** ermöglicht die Sortierung der angezeigten Informationen nach Datum, Anforderer, Anforderungsempfänger oder Anforderungstyp.

Um auf die Seite ″Beendete Anforderungen″ zuzugreifen, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie auf **Beendete Anforderungen anzeigen**.

Persönliche Informationen

Der Bereich ″Persönliche Informationen″ enthält Informationen über Sie als den Eigner von Accounts, die von Tivoli Identity Manager verwaltet werden.

Das Formular ″Persönliche Informationen″ kann von einem Systemadministrator individuell angepasst werden. Das Standardformular ″Persönliche Informationen″ enthält eine Auflistung der folgenden Angaben:

Registerkarte	Feld	Beschreibung
Persönliche Informationen	Nachname	Nachname des Accounteigners.
	Vollständiger Name	Vollständiger Name des Accounteigners. Diese Angabe dient dazu, den Accounteigner in einer Auflistung mehrerer Personen eindeutig zu identifizieren.
	Vorname	Vorname des Accounteigners.
	Initialen	Initialen des Accounteigners.
	Privatadresse	Privatadresse des Accounteigners.
	Shared Secret	Kennwort für den Accounteigner zum Abrufen des Kennworts für einen neuen Account. Dieser Wert ist erforderlich, wenn das Tivoli Identity Manager Server-System das Erstkennwort für den Account generiert.
	Organisationsberechtigungsklassen	Organisationsberechtigungsklassen, denen der Accounteigner angehört.
Firmeninformationen	Zimmernummer	Arbeitsplatznummer des Accounteigners (die normalerweise aus einer graphischen Arbeitsplatzübersicht stammt).
	Personalnummer	Personalnummer des Accounteigners.
	Titel	Jobbezeichnung des Accounteigners.
	Vorgesetzter	Direkter Vorgesetzter des Accounteigners.
	Postadresse	Firmenanschrift des Accounteigners.
	Sekretär/in	Name der Sekretärin oder des Sekretärs (sofern zutreffend) des Accounteigners.
Kontaktinformationen	E-Mail-Adresse	E-Mail-Adresse des Accounteigners (normalerweise eine Kombination aus der Vornamensinitiale und dem Nachnamen des Accounteigners). Diese Adresse wird vom System dazu verwendet, den Accounteigner über Anforderungen und sonstige Aktionen zu informieren.
	Telefonnummer	Bürotelefonnummer des Accounteigners.
	Mobiltelefonnummer	Telefonnummer des Firmenmobiltelefons des Accounteigners.
	Pagernummer	Telefonnummer des Firmenpagers des Accounteigners.
	Telefonnummer (privat)	Private Telefonnummer des Accounteigners.
	Aliasnamen	Zusätzliche Aliasnamen, die vom Accounteigner verwendet werden. Dieses Attribut wird von Tivoli Identity Manager zum Abgleichen der Benutzer-IDs des Accounts auf verwalteten Ressourcen.

Um persönliche Informationen einzugeben, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Auf persönliche Informationen zugreifen**.
   Die Seite ″Auf persönliche Informationen zugreifen″ wird geöffnet.
3. Nehmen Sie die gewünschten Änderungen auf den Registerkarten ″Persönliche Informationen″, ″Firmeninformationen″ und ″Kontaktinformationen″ vor.
4. Klicken Sie auf **Übergeben**.

Anmerkung: Organisationsberechtigungsklassen können auf der Seite ″Persönliche Informationen″ hinzugefügt werden. Hierdurch wird der Zugriff auf verwaltete Ressourcen übertragen, die durch die Zugehörigkeit zu einer Organisationsberechtigungsklasse zulässig sind.

Delegieren von Berechtigungen

Die Seite ″Berechtigung delegieren″ dient dazu, Personen zu bestimmen, denen Sie ihre Genehmigungsberechtigung übertragen wollen. Diese Funktion wird bei der Anforderungsgenehmigung verwendet und dient dazu, im Rahmen eines Verarbeitungsschritts bei der Anforderungseinrichtung Informationen zur Verfügung zu stellen.

Sie können mehrere Stellvertreter auswählen, wobei jedoch immer nur ein Stellvertreter für einen gegebenen Zeitraum angegeben werden kann. Wenn Sie die Person ändern wollen, die Sie für einen bestimmten Zeitraum als Stellvertreter festgelegt haben, müssen Sie die ursprünglich für diese Funktion angegebene Person löschen und eine neue Person für den ausgewählten Zeitraum hinzufügen.

Hinzufügen eines Stellvertreters

Um eine Berechtigung zu delegieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Berechtigung delegieren**.
   Die Seite ″Berechtigung delegieren″ wird geöffnet.
3. Klicken Sie auf **Hinzufügen**.
4. Suchen Sie mit Hilfe der Suchfunktion die gewünschte Person, wählen Sie das Markierungsfeld neben dem Namen dieser Person aus, und klicken Sie anschließend auf **Hinzufügen**.
5. Wählen Sie ein Start- und ein Enddatum für die Delegierung der Genehmigungsberechtigung aus, die an die ausgewählte Person übertragen wird.
6. Klicken Sie auf **Übergeben**.

Wechseln des Stellvertreters

Um die Person zu wechseln, die Sie für einen bestimmten Zeitraum als Stellvertreter festgelegt haben, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Berechtigung delegieren**.

3. Wählen Sie das Markierungsfeld neben dem Namen des angegebenen Stellvertreters aus, und klicken Sie anschließend auf **Löschen**.

   Die Seite ″Löschen bestätigen″ wird geöffnet.
4. Klicken Sie auf **Übergeben**.

   Der Stellvertreter wird aus der Liste der Stellvertreter entfernt.
5. Verwenden Sie die unter ″Hinzufügen eines Stellvertreters″ beschriebene Prozedur, um einen neuen Stellvertreter für den betreffenden Zeitraum hinzuzufügen.

Ändern des ausgewählten Stellvertreters

Um den Delegationszeitraum für einen vorhandenen Stellvertreter zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Berechtigung delegieren**.
3. Klicken Sie auf den Namen der Person, für die Sie Änderungen vornehmen wollen.
4. Ändern Sie die Datumsangaben für das Start- und Enddatum wie gewünscht.
5. Klicken Sie auf **Übergeben**.

Antworten auf Kennwortprüffragen des Challenge/Response-Verfahrens

ITIM-Benutzer können ihre Antworten auf die Kennwortprüffragen des Challenge/Response-Verfahrens jederzeit ändern. Wenn beim Challenge/Response-Verfahren mehrere Kennwortprüffragen beantwortet werden müssen, ist es möglich, nur eine Antwort zu ändern und die übrigen Antworten unverändert zu lassen.

Diese Funktion ist standardmäßig inaktiviert. Wird diese Option ausgewählt, während die Funktion inaktiviert ist, wird auf der Seite eine Nachricht angezeigt, die darüber informiert, dass diese Funktion gegenwärtig inaktiviert ist. Wenn diese Funktion jedoch aktiviert ist, können die Antworten auf Kennwortprüffragen im Challenge/Response-Verfahren mit Hilfe der nachstehenden Prozeduren geändert werden.

Um Antworten auf Kennwortprüffragen des Challenge/Response-Verfahrens zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Ausgangsposition**.
2. Klicken Sie in der Taskleiste auf **Antwort auf Kennwortprüffrage definieren**.

   Die Seite ″Antwort auf Prüffrage″ wird geöffnet.
3. Ändern Sie die Antworten auf die entsprechenden Kennwortprüffragen des Challenge/Response-Verfahrens, und klicken Sie anschließend auf **Übergeben**.

   Die Änderungen der Antworten auf die Kennwortprüffragen des Challenge/Response-Verfahrens werden gespeichert.

Kapitel 5. Berichte

Ein Benutzer mit entsprechender Berechtigung kann das Tivoli Identity Manager-Berichtssystem zum Erstellen von Berichten anhand ausgewählter Kriterien verwenden. Tivoli Identity Manager ermöglicht berechtigten Benutzern, die folgenden Berichtstypen zu generieren:

- Operation
- Service
- Benutzer
- Zurückgewiesen
- Datenabgleich
- Ruhend
- Account
- Ad-hoc

Wichtig: Damit Sie die Berichte anzeigen können, muss Adobe Acrobat Reader™ installiert sein. Alle Berichte werden im PDF-Dateiformat erstellt. Darüber hinaus muss Internet Explorer Version 5.5 mit Service-Pack 2 oder höher bzw. Netscape Version 4.75 vorhanden sein.

Berichtstypen

Die folgende Tabelle enthält eine Auflistung der in Tivoli Identity Manager verfügbaren Berichtstypen mit den zugehörigen Beschreibungen. Die Berichte, die für einen bestimmten Benutzer zur Verfügung stehen, hängen jedoch von der jeweiligen ITIM-Gruppe ab, der der Benutzer angehört.

Berichtsname	Beschreibung
Operation	Listet die Operationsanforderungen in Tivoli Identity Manager nach Operationstyp, Operationsdatum, Anforderer der Operation und Empfänger der angeforderten Operation auf. Für diesen Bericht können die folgenden Parameter definiert werden: • Anforderer • Anforderungsempfänger • Operationen • Startdatum • Enddatum
Service	Listet die vorhandenen Serviceinstanzen nach Datum, Anforderer der Operation und Empfänger der angeforderten Operation auf. Für diesen Bericht können die folgenden Parameter definiert werden: • Anforderer • Anforderungsempfänger • Serviceinstanz • Startdatum • Enddatum

Berichtsname	Beschreibung
Benutzer	Listet alle Operationen in Tivoli Identity Manager nach Datum, Anforderer der Operation und Empfänger der angeforderten Operation auf. Für diesen Bericht können die folgenden Parameter definiert werden: • Anforderer • Anforderungsempfänger • Startdatum • Enddatum
Zurückgewiesen	Listet die zurückgewiesenen (verweigerten) Anforderungen nach Datum, Anforderer der Operation und Empfänger der angeforderten Operation auf. Für diesen Bericht können die folgenden Parameter definiert werden: • Serviceinstanz
Datenabgleich	Listet die Waisenaccounts auf, die seit der Ausführung des letzten Datenabgleichs gefunden wurden. Für diesen Bericht können die folgenden Parameter definiert werden: • Serviceinstanz
Ruhend	Listet die Services ohne Aktivität innerhalb des ausgewählten Zeitraums (in Tagen) auf. Für diesen Bericht können die folgenden Parameter definiert werden: • Serviceinstanz • Anzahl von Tagen, die der Service geruht hat
Account	Listet Personen und die ihnen zugeordneten Accounts auf und gibt an, ob der Account mit den Regeln der aktuellen Richtlinien konform ist. Für diesen Bericht können die folgenden Parameter definiert werden: • Serviceinstanz • Anzahl von Tagen, die der Service geruht hat
Ad-hoc	Die Berichte, die von den angegebenen Berichtdesignern entworfen/importiert wurden.

Die folgende Auflistung enthält alle Berichte, die für eine spezifische Serviceinstanz ausgeführt werden können:

- Service
- Datenabgleich
- Ruhend
- Account
- Ad-hoc

In den folgenden Abschnitten werden die unterschiedlichen Berichtstypen im Detail beschrieben.

Berichte für Endbenutzer

Generell kann jeder Benutzer, der über einen ITIM-Account verfügt, Berichte anzeigen. Dazu muss der ITIM-Gruppe des Benutzers jedoch zuvor anhand einer Bericht-ACI der Zugriff auf mindestens einen bestimmten Bericht erteilt werden. Benutzer können darüber hinaus alle angepassten Berichte anzeigen, für die sie die entsprechenden Anzeigeberechtigungen besitzen. Die Anzahl der Berichte, die verschiedenen Benutzern zur Verfügung stehen, kann begrenzt werden, indem spezielle Bericht-ACIs so definiert werden, dass sie den Zugriff auf bestimmte Berichtstypen explizit erteilen oder verweigern.

Ein Endbenutzer kann nur einen Bericht der Aktivität anzeigen, die für ihn entweder als Anforderungsempfänger oder als Anforderer spezifisch ist. Ein Manager beispielsweise kann Berichte für Anforderungen anzeigen, die von ihm eingeleitet wurden oder die für ihn gestellt wurden. Ein Mitarbeiter ohne die entsprechende Position eines Managers oder Vorgesetzten hingegen kann Berichte nur für diejenigen Anforderungen anzeigen, die für ihn gestellt wurden, da er keine Anforderungen einleiten kann.

Bericht ″Operation″

Der Bericht ″Operation″ zeigt an, welche Tivoli Identity Manager-Operationen angefordert wurden, von wem diese Operationen angefordert wurden und für wen diese Operationen angefordert wurden. Der Bericht kann Anforderungen für eine spezifische Operation wahlweise für alle Systembenutzer oder aber einen bestimmten Systembenutzer anzeigen. Darüber hinaus können Sie anfordern, dass der Bericht alle Personen anzeigt, für die die Operation ausgeführt werden sollte, oder Sie wählen nur eine Person aus und zeigen die Anforderungen für die ausgewählte Operation an, die ausgeführt werden sollte. Darüber hinaus können Sie einen Datumsbereich eingeben, sodass nur Operationsanforderungen innerhalb des angegebenen Zeitraums angezeigt werden.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können:

Anforderer	Der Anforderer ist der Benutzer, der die Anforderung eingeleitet hat. Wird kein Anforderer ausgewählt, durchsucht Tivoli Identity Manager alle Systembenutzer nach dem ausgewählten Service.
Anforderungsempfänger	Der Anforderungsempfänger ist der Benutzer, der hinzugefügt, geändert oder gelöscht wird. Wird kein Anforderungsempfänger ausgewählt, durchsucht Tivoli Identity Manager alle Personen nach dem ausgewählten Service. **Anmerkung:** Tivoli Identity Manager durchsucht nur Personen, für die eine vorhandene Instanz des ausgewählten Services in Kraft ist.

Operation	Der Operationstyp, nach dem Tivoli Identity Manager beim Generieren des Berichts sucht. **Erforderlich**. Folgende Operationstypen sind verfügbar: • Neuer Benutzer • Serviceeinrichtung • Änderung des Accountkennworts • Account aussetzen • Account wiederherstellen • Account löschen • Änderung von Benutzerdaten • Änderung der Unternehmensbereichs des Benutzers • Benutzer aussetzen • Benutzer wiederherstellen • Benutzer löschen • Account ändern
Start-/Enddatum und Uhrzeit	Zeit- und Datumsbereich, auf den der Bericht beschränkt ist. Der Bericht enthält in diesem Fall nur Serviceinstanzen, die innerhalb des ausgewählten Datums- und Zeitbereichs aktiv sind.

Um einen Bericht des Typs "Operation" zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.
   Die Seite "Menü 'Berichte'" wird geöffnet.
3. Klicken Sie auf **Bericht 'Operation'**.
   Die Seite "Bericht 'Operation' - Suche" wird geöffnet.
4. **OPTIONAL:** Wählen Sie einen Anforderer aus.
   a. Klicken Sie auf **...ITIM-Benutzer abrufen**.
      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.
      Die Seite "Suchfilter - Ergebnisse" wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen des gewünschten Benutzers aus, und klicken Sie auf **Hinzufügen**.
      Die Seite "Bericht 'Operation' - Suche" wird erneut angezeigt, und der ausgewählte Anforderer ist jetzt im Feld **Anforderer** enthalten.
5. **OPTIONAL:** Wählen Sie einen Anforderungsempfänger aus.
   a. Klicken Sie auf **...Person abrufen**.
      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.

c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

   Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
f. Wählen Sie den Radioknopf neben dem Namen der gewünschten Person aus, und klicken Sie auf **Hinzufügen**.

   Die Seite ″Bericht 'Operation' - Suche″ wird erneut angezeigt, und der ausgewählte Anforderungsempfänger ist jetzt im Feld **Anforderungsempfänger** enthalten.

6. Wählen Sie im Dropdown-Menü **Operationen** einen Operationstyp aus.
7. Wählen Sie das Start- und das Enddatum sowie die Start- und die Endzeit aus. Wählen Sie hierzu aus den entsprechenden Dropdown-Menüs das Jahr, den Monat und den Tag sowie die Uhrzeit aus.
8. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
9. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters ″Bericht″ auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht ″Service″

Der Bericht ″Service″ listet auf der Grundlage der übrigen Berichtauswahlkriterien die vorhandenen Serviceinstanzen auf, die in Kraft sind. Im Bericht werden nur diejenigen Serviceinstanzen angezeigt, die vom ausgewählten Systembenutzer (oder ALLEN Systembenutzern) angefordert wurden, sowie die Serviceinstanzen, die für die ausgewählte Person (oder ALLE Personen) aktiv sind und in den Datums-/Zeitbereich fallen.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können:

Anforderer	Der Anforderer ist der Benutzer, der die Anforderung eingeleitet hat. Wird kein Anforderer ausgewählt, durchsucht Tivoli Identity Manager alle Systembenutzer nach dem ausgewählten Service.
Anforderungsempfänger	Der Anforderungsempfänger ist der Benutzer, der hinzugefügt, geändert oder gelöscht wird. Wird kein Anforderungsempfänger ausgewählt, durchsucht Tivoli Identity Manager alle Personen nach dem ausgewählten Service. **Anmerkung:** Tivoli Identity Manager durchsucht nur Personen, für die eine vorhandene Instanz des ausgewählten Services in Kraft ist.
Serviceinstanz	**Erforderlich.** Eine Serviceinstanz ist ein Service, der in Tivoli Identity Manager oder einer einzelnen Instanz eines Services verfügbar ist, wenn der Service mehrere Instanzen aufweist.

Start-/Enddatum und Uhrzeit	Zeit- und Datumsbereich, auf den der Bericht beschränkt ist. Der Bericht enthält in diesem Fall nur Serviceinstanzen, die innerhalb des ausgewählten Datums- und Zeitbereichs aktiv sind.

Um einen Bericht des Typs "Service" zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.

   Die Seite "Menü 'Berichte'" wird geöffnet.
3. Klicken Sie auf **Bericht 'Service'**.

   Die Seite "Bericht 'Service' - Suche" wird geöffnet.
4. **OPTIONAL:** Wählen Sie einen Anforderer aus.
   a. Klicken Sie auf **...ITIM-Benutzer abrufen**.

      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite "Suchfilter - Ergebnisse" wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen des gewünschten Benutzers aus, und klicken Sie auf **Hinzufügen**.

      Die Seite "Bericht 'Service' - Suche" wird erneut angezeigt, und der ausgewählte Anforderer ist jetzt im Feld **Anforderer** enthalten.
5. **OPTIONAL:** Wählen Sie einen Anforderungsempfänger aus.
   a. Klicken Sie auf **...Person abrufen**.

      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite "Suchfilter - Ergebnisse" wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen der gewünschten Person aus, und klicken Sie auf **Hinzufügen**.

      Die Seite "Bericht 'Service' - Suche" wird erneut angezeigt, und der ausgewählte Anforderungsempfänger ist jetzt im Feld **Anforderungsempfänger** enthalten.
6. Wählen Sie eine Serviceinstanz aus.
   a. Klicken Sie auf **...Service abrufen**.

      Die Seite "Service - Suche" wird geöffnet.
   b. Wählen Sie im Dropdown-Menü **Profil auswählen** ein Serviceprofil aus.
   c. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   d. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.

e. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
f. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

   Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
g. Wählen Sie den Radioknopf neben dem Namen des gewünschten Services aus, und klicken Sie auf **Hinzufügen**.

   Die Seite ″Bericht 'Service' - Suche″ wird erneut angezeigt, und der ausgewählte Service ist jetzt im Feld **Serviceinstanz** enthalten.

7. Wählen Sie das Start- und das Enddatum sowie die Start- und die Endzeit aus. Wählen Sie hierzu aus den entsprechenden Dropdown-Menüs das Jahr, den Monat und den Tag sowie die Uhrzeit aus.
8. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
9. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters ″Bericht″ auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht ″Benutzer″

Der Bericht ″Benutzer″ listet alle Tivoli Identity Manager-Operationen auf, die angefordert wurden, und zeigt darüber hinaus an, von wem diese Operationen angefordert wurden und für wen diese Operationen angefordert wurden. Sie können auswählen, ob die Anforderungen für alle Systembenutzer oder aber nur für einen bestimmten Systembenutzer angezeigt werden sollen. Darüber hinaus können Sie anfordern, dass der Bericht alle Personen anzeigt, für die die Operation ausgeführt werden sollte, oder Sie wählen nur eine Person aus und zeigen alle Anforderungen für diese Person von allen Systembenutzern an oder zeigen diese nur von einem ausgewählten Systembenutzer an. Darüber hinaus können Sie einen Datumsbereich eingeben, sodass nur Operationsanforderungen innerhalb des angegebenen Zeitraums angezeigt werden.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können.

Anforderer	Der Anforderer ist der Benutzer, der die Anforderung eingeleitet hat. Wird kein Anforderer ausgewählt, durchsucht Tivoli Identity Manager alle Systembenutzer nach dem ausgewählten Service.
Anforderungsempfänger	Der Anforderungsempfänger ist der Benutzer, der hinzugefügt, geändert oder gelöscht wird. Wird kein Anforderungsempfänger ausgewählt, durchsucht Tivoli Identity Manager alle Personen nach dem ausgewählten Service. **Anmerkung:** Tivoli Identity Manager durchsucht nur Personen, für die eine vorhandene Instanz des ausgewählten Services in Kraft ist.
Start-/Enddatum und Uhrzeit	Zeit- und Datumsbereich, auf den der Bericht beschränkt ist. Der Bericht enthält in diesem Fall nur Serviceinstanzen, die innerhalb des ausgewählten Datums- und Zeitbereichs aktiv sind.

Um einen Bericht des Typs ″Benutzer″ zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.

   Die Seite ″Menü 'Berichte'″ wird geöffnet.
3. Klicken Sie auf **Bericht 'Benutzer'**.

   Die Seite ″Bericht 'Benutzer' - Suche″ wird geöffnet.
4. **OPTIONAL:** Wählen Sie einen Anforderer aus.
   a. Klicken Sie auf **...ITIM-Benutzer abrufen**.

      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen des gewünschten Benutzers aus, und klicken Sie auf **Hinzufügen**.

      Die Seite ″Bericht 'Benutzer' - Suche″ wird erneut angezeigt, und der ausgewählte Anforderer ist jetzt im Feld **Anforderer** enthalten.
5. **OPTIONAL:** Wählen Sie einen Anforderungsempfänger aus.
   a. Klicken Sie auf **...Person abrufen**.

      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen der gewünschten Person aus, und klicken Sie auf **Hinzufügen**.

      Die Seite ″Bericht 'Benutzer' - Suche″ wird erneut angezeigt, und der ausgewählte Anforderungsempfänger ist jetzt im Feld **Anforderungsempfänger** enthalten.
6. Wählen Sie das Start- und das Enddatum sowie die Start- und die Endzeit aus. Wählen Sie hierzu aus den entsprechenden Dropdown-Menüs das Jahr, den Monat und den Tag sowie die Uhrzeit aus.
7. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
8. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters ″Bericht″ auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht ″Zurückgewiesen″

Der Bericht ″Zurückgewiesen″ listet alle Tivoli Identity Manager-Anforderungen auf, die zurückgewiesen wurden. Sie können wahlweise alle zurückgewiesenen Operationen anzeigen lassen oder aber bestimmte Systembenutzer auswählen, damit nur die Operationen angezeigt werden, die für den jeweils ausgewählten Systembenutzer zurückgewiesen wurden. Darüber hinaus können Sie auch angeben, dass nur Operationen angezeigt werden sollen, die für eine bestimmte Person zurückgewiesen wurden, für die die Operationen ausgeführt werden sollten. Unabhängig vom ausgewählten Operationstyp werden in beiden Fällen alle Tivoli Identity Manager-Operationen angezeigt, die den festgelegten Kriterien für Anforderer bzw. Anforderungsempfänger entsprechen.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können:

Anforderer	Der Anforderer ist der Benutzer, der die Anforderung eingeleitet hat. Wird kein Anforderer ausgewählt, durchsucht Tivoli Identity Manager alle Systembenutzer nach dem ausgewählten Service.
Anforderungsempfänger	Der Anforderungsempfänger ist der Benutzer, der hinzugefügt, geändert oder gelöscht wird. Wird kein Anforderungsempfänger ausgewählt, durchsucht Tivoli Identity Manager alle Personen nach dem ausgewählten Service. **Anmerkung:** Tivoli Identity Manager durchsucht nur Personen, für die eine vorhandene Instanz des ausgewählten Services in Kraft ist.
Start-/Enddatum und Uhrzeit	Zeit- und Datumsbereich, auf den der Bericht beschränkt ist. Der Bericht enthält in diesem Fall nur Serviceinstanzen, die innerhalb des ausgewählten Datums- und Zeitbereichs aktiv sind.

Um einen Bericht des Typs ″Zurückgewiesen″ zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.
   Die Seite ″Menü 'Berichte'″ wird geöffnet.
3. Klicken Sie auf **Bericht 'Zurückgewiesen'**.
   Die Seite ″Bericht 'Zurückgewiesen' - Suche″ wird geöffnet.
4. **OPTIONAL:** Wählen Sie einen Anforderer aus.
   a. Klicken Sie auf **...ITIM-Benutzer abrufen**.
      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.
      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.

f. Wählen Sie den Radioknopf neben dem Namen des gewünschten Benutzers aus, und klicken Sie auf **Hinzufügen**.

   Die Seite "Bericht 'Zurückgewiesen' - Suche" wird erneut angezeigt, und der ausgewählte Anforderer ist jetzt im Feld **Anforderer** enthalten.

5. **OPTIONAL:** Wählen Sie einen Anforderungsempfänger aus.
   a. Klicken Sie auf **...Person abrufen**.

      Die Suchseite für Benutzer wird geöffnet.
   b. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite "Suchfilter - Ergebnisse" wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen der gewünschten Person aus, und klicken Sie auf **Hinzufügen**.

      Die Seite "Bericht 'Zurückgewiesen' - Suche" wird erneut angezeigt, und der ausgewählte Anforderungsempfänger ist jetzt im Feld **Anforderungsempfänger** enthalten.
6. Wählen Sie das Start- und das Enddatum sowie die Start- und die Endzeit aus. Wählen Sie hierzu aus den entsprechenden Dropdown-Menüs das Jahr, den Monat und den Tag sowie die Uhrzeit aus.
7. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
8. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters "Bericht" auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht "Datenabgleich"

Der Bericht "Datenabgleich" listet die folgenden Informationen auf:

- Anzahl der erstellten Waisenaccounts
- Anzahl der erstellten Accounts mit Eigner
- Anzahl der aktualisierten Accounts
- Anzahl der entfernten lokalen Accounts
- Gesamtzahl aller verarbeiteten Accounts
- Detaillierte Auflistung der geänderten Personen und Accounts

Um einen Bericht des Typs "Datenabgleich" zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.

   Die Seite "Menü 'Berichte'" wird geöffnet.

3. Klicken Sie auf **Bericht 'Datenabgleich'**.
   Die Seite "Bericht 'Datenabgleich' - Suche" wird geöffnet.
4. Wählen Sie eine Serviceinstanz aus.
   a. Klicken Sie auf **...Service abrufen**.
      Die Seite "Service - Suche" wird geöffnet.
   b. Wählen Sie im Dropdown-Menü **Profil auswählen** ein Serviceprofil aus.
   c. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   d. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   e. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   f. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.
      Die Seite "Suchfilter - Ergebnisse" wird geöffnet.
   g. Wählen Sie den Radioknopf neben dem Namen des gewünschten Services aus, und klicken Sie auf **Hinzufügen**.
      Die Seite "Bericht 'Datenabgleich' - Suche" wird erneut angezeigt, und der ausgewählte Service ist jetzt im Feld **Serviceinstanz** enthalten.
5. Klicken Sie auf **Übergeben**.
   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
6. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters "Bericht" auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht "Ruhend"

Der Bericht "Ruhend" listet alle Accounts für den angegebenen Service auf, die innerhalb des in Tagen angegebenen Zeitraums nicht benutzt oder noch nie benutzt wurden.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können.

Serviceinstanz	**Erforderlich.** Eine Serviceinstanz ist ein Service, der in Tivoli Identity Manager oder einer einzelnen Instanz eines Services verfügbar ist, wenn der Service mehrere Instanzen aufweist.
Hat über folgenden Zeitraum (in Tagen) geruht	**Erforderlich.** Der Zeitraum in Tagen, den ein Account für den ausgewählten Service geruht hat.

Um einen Bericht des Typs "Ruhend" zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.
   Die Seite "Menü 'Berichte'" wird geöffnet.
3. Klicken Sie auf **Bericht 'Ruhend'**.
   Die Seite "Bericht 'Ruhend' - Suche" wird geöffnet.

4. Wählen Sie eine Serviceinstanz aus.
   a. Klicken Sie auf **...Service abrufen**.

      Die Seite ″Service - Suche″ wird geöffnet.
   b. Wählen Sie im Dropdown-Menü **Profil auswählen** ein Serviceprofil aus.
   c. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   d. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   e. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   f. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
   g. Wählen Sie den Radioknopf neben dem Namen des gewünschten Services aus, und klicken Sie auf **Hinzufügen**.

      Die Seite ″Bericht 'Ruhend' - Suche″ wird erneut angezeigt, und der ausgewählte Service ist jetzt im Feld **Serviceinstanz** enthalten.
5. Geben Sie den Zeitraum in Tagen, den der Account geruht hat und nach dem gesucht werden soll, in das Textfeld **Hat über folgenden Zeitraum (in Tagen) geruht:** ein.
6. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
7. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters ″Bericht″ auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Bericht ″Account″

Der Bericht ″Account″ listet die Personen und die ihnen zugeordneten Accounts auf und gibt an, ob ein Account mit den aktuellen Richtlinien für den angegebenen Unternehmensbereich und seine untergeordneten Einheiten konform ist.

Die folgende Tabelle erläutert die Suchfelder, auf die Berichte begrenzt werden können.

Serviceinstanz	**Erforderlich.** Eine Serviceinstanz ist ein Service, der in Tivoli Identity Manager oder einer einzelnen Instanz eines Services verfügbar ist, wenn der Service mehrere Instanzen aufweist.
Unternehmensbereich	**Erforderlich.** Der Unternehmensbereich ist das Kriterium, nach dem die Benutzer und die ihnen zugeordneten Accounts aufgelistet werden. Folgende Typen von Unternehmensbereichen können angegeben werden: • Verwaltungsdomäne • Geschäftspartnerorganisation • Standort • Organisation • Organisationseinheit

Um einen Bericht des Typs ″Account″ zu generieren, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.

   Die Seite ″Menü 'Berichte'″ wird geöffnet.
3. Klicken Sie auf **Bericht 'Account'**.

   Die Seite ″Bericht 'Account' - Suche″ wird geöffnet.
4. Wählen Sie eine Serviceinstanz aus.
   a. Klicken Sie auf **...Service abrufen**.

      Die Seite ″Service - Suche″ wird geöffnet.
   b. Wählen Sie im Dropdown-Menü **Profil auswählen** ein Serviceprofil aus.
   c. Wählen Sie das Markierungsfeld **Nur ausgewählte Organisation** aus, damit die Suche nur innerhalb der ausgewählten Organisation ausgeführt wird.
   d. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   e. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Suchfilter aus.
   f. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
   g. Wählen Sie den Radioknopf neben dem Namen des gewünschten Services aus, und klicken Sie auf **Hinzufügen**.

      Die Seite ″Bericht 'Account' - Suche″ wird erneut angezeigt, und der ausgewählte Service ist jetzt im Feld **Serviceinstanz** enthalten.
5. Wählen Sie einen Unternehmensbereich aus.
   a. Klicken Sie auf **...Unternehmensbereich abrufen**.

      Die Seite ″Suche″ wird geöffnet.
   b. Wählen Sie Dropdown-Menü **Typ auswählen** einen Unternehmensbereichstyp aus.
   c. Wählen Sie im Dropdown-Menü **Suchattribut** ein Suchattribut aus.
   d. Wählen Sie im Dropdown-Menü **Ausdruck auswählen** einen Ausdruck aus.
   e. Geben Sie einen Suchparameter in das Textfeld ein, und klicken Sie auf **Suchen**.

      Die Seite ″Suchfilter - Ergebnisse″ wird geöffnet.
   f. Wählen Sie den Radioknopf neben dem Namen des gewünschten Services aus, und klicken Sie auf **Weiter**.

      Die Seite ″Bericht 'Account' - Suche″ wird erneut angezeigt, und der ausgewählte Unternehmensbereich ist jetzt im Feld **Unternehmensbereich** enthalten.
6. Klicken Sie auf **Übergeben**.

   Basierend auf den ausgewählten Suchkriterien wird ein Bericht generiert. Der Bericht wird mit Adobe Acrobat Reader angezeigt.
7. Um den Bericht in PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters ″Bericht″ auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.

Ad-hoc-Berichte (und Crystal Reports-Berichte)

Schablonen für Ad-hoc-Berichte werden entweder mit Hilfe der eingebetteten Berichtdesignfunktion (Report Designer) erstellt oder von einer Berichtdesignfunktion anderer Lieferanten (beispielsweise Crystal Reports) importiert. Ad-hoc-Berichte werden anschließend direkt über die Benutzerschnittstelle von Tivoli Identity Manager ausgeführt.

Systemadministratoren können Berichte konzipieren, die speziell an die Bedürfnisse einer Organisation angepasst sind. Die in Ad-hoc-Berichten enthaltenen Anzeigefelder hängen dabei jeweils vom Aufbau des Berichts ab.

Um einen Ad-hoc-Bericht zu generieren und zu speichern, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste des Hauptmenüs auf **Bericht**.
2. Klicken Sie in der Taskleiste auf **Bericht ausführen**.
   Die Seite "Menü 'Berichte'" wird geöffnet.
3. Wählen Sie den angepassten Bericht aus der Liste aus.
4. Geben Sie das Berichtsformat (PDF/CSV) an.

   Anmerkung: Diese Option wird für Berichte angezeigt, die mit Hilfe der Ad-hoc-Berichtsschnittstelle von Tivoli Identity Manager entworfen wurden.
5. Führen Sie gegebenenfalls die zum Generieren des Berichts erforderlichen Eingaben durch.

   Anmerkung: Bei Ad-hoc-Berichten von Tivoli Identity Manager muss die Benutzereingaben den Syntaxregeln für SQL-Abfragen entsprechen. Um beispielsweise die Namen aller Personen abzurufen, die mit dem Buchstaben J beginnen, muss die Benutzereingabe J% lauten und nicht J*.

   Anmerkung: Bei Crystal-Berichten muss die Benutzereingabe der Standardsyntax für reguläre Ausdrücke entsprechen. Um beispielsweise die Namen aller Personen abzurufen, die mit dem Buchstaben **J** beginnen, muss die Benutzereingabe **J*** lauten.
6. Klicken Sie auf **Übergeben**.
   Es wird eine Bericht generiert und in dem ausgewählten Format angezeigt.
7. Um den Ad-hoc-Bericht im PDF-Format auf dem Clientsystem zu speichern, klicken Sie in der Funktionsleiste des Fensters "Bericht" auf das Symbol **Speichern**. In einigen Fällen kann es vorkommen, dass der Standarddateiname, der im Feld **Dateiname** angezeigt wird, nicht gültig ist (zu viele Zeichen). Wechseln Sie in das Verzeichnis, in dem Sie die Datei sichern wollen, und geben Sie in das Feld **Dateiname** einen gültigen Dateinamen ein. Klicken Sie auf **Speichern**.
   Um einen Crystal-Bericht in einem der unterstützten Formate auf dem Clientsystem zu speichern, exportieren Sie den Crystal-Bericht mit Hilfe der Option **Exportieren** auf der Seite mit der Berichtsausgabe. Klicken Sie anschließend auf **Speichern**, um den Bericht zu speichern.

Glossar

A

Abfrage. Ein Verfahren, mit dem die Ausführung eines Datenabgleichs begrenzt wird, sodass kleinere Pakete zurückgegeben werden.

Ablaufzeitraum für Kennwörter. Die Zeitspanne, in der ein Kennwort verwendet werden kann, bevor es vom Benutzer geändert werden muss.

Account. Die Parametermenge, die die Anmeldeinformationen und die Zugriffssteuerungsinformationen für einen Benutzer definiert.

Aktiver Account. Ein Account, der vorhanden ist und vom Eigner für den Zugriff auf eine Ressource verwendet wird.

Aliasname. Eine Identität für einen Benutzer, die in der Regel als Benutzer-ID bezeichnet wird. Eine Person kann über mehrere Aliasnamen verfügen, zum Beispiel ″GSmith″ und ″GWSmith″.

Anforderer. Eine Person, die eine Anforderung übergibt.

Anforderung. Ein Aktionselement im Tivoli Identity Manager-System, das eine Anfrage für eine Genehmigung oder für Informationen stellt.

Anforderungsempfänger. Die Person, für die eine Anforderung übergeben wird.

Anstehende Anforderungen. Anforderungen, die an das System übergeben wurden, aber noch nicht verarbeitet und beendet wurden.

Arbeitsablauf. Die Reihenfolge der Aktionen, die im Einklang mit den Geschäftsprozessen eines Unternehmens ausgeführt werden.

Aussetzen. Die Inaktivierung eines Accounts, sodass sich der Accounteigner nicht mehr bei der Ressource anmelden kann.

Authentifizierung. Der Prozess der Identifizierung einer Einzelperson. Diese erfolgt in der Regel anhand eines Benutzernamens und eines Kennworts. Bei Sicherheitssystemen unterscheidet sich die Authentifizierung von der Berechtigung insofern, als dass die Berechtigung die Erteilung von Zugriffsrechten auf Systemobjekte auf der Basis der Identität des Benutzers darstellt. Die Authentifizierung stellt lediglich sicher, dass es sich bei der Einzelperson tatsächlich um die Person handelt, als die diese sich ausgibt, besitzt jedoch keinerlei Aussagekraft hinsichtlich der Zugriffsberechtigungen dieser Einzelperson.

B

Beendete Anforderungen. Anforderungen, die an das System übergeben wurden und deren Bearbeitung vollständig abgeschlossen und beendet wurde.

Benutzer. Jede beliebige Person, die mit dem System interagiert.

Benutzername. Die ID, die der Benutzer für den Zugriff auf das System verwendet. Diese ID identifiziert darüber hinaus den Benutzer beim System und ermöglicht dem System, die Zugriffsberechtigungen des Benutzers auf der Basis seiner Zugehörigkeit zu den verschiedenen Organisationsberechtigungsklassen und ITIM-Gruppen zu ermitteln.

Benutzerschnittstelle (UI). Die Anzeige, die der Benutzer für die Interaktion mit dem System verwendet.

Berechtigung. Bei der Absicherung von Computern und Computersystemen das einem Benutzer erteilte Recht zum Kommunizieren mit oder Nutzen von einem Computersystem. Hierbei ist der Prozess gemeint, bei dem einem Benutzer der vollständige oder eingeschränkte Zugriff auf ein Objekt, eine Ressource oder eine Funktion erteilt wird.

Die meisten Computersicherheitssysteme basieren auf einem Prozess, der aus zwei Stufen aufgebaut ist. In einer ersten Stufe erfolgt die Authentifizierung, mit deren Hilfe sichergestellt wird, dass ein Benutzer tatsächlich die Person ist, die er zu sein vorgibt. In der zweiten Stufe erfolgt die Berechtigung, die dem Benutzer - basierend auf seiner Benutzeridentität - den Zugriff auf verschiedene Ressourcen erteilt.

Berechtigungsnachweis. Die Benutzer-ID und die Kennwortinformationen für einen Benutzer, die den Zugriff auf einen Account ermöglichen.

Bericht ″Account″. Ein Bericht, der Personen und die ihnen zugeordneten Accounts auflistet und angibt, ob der Account mit den aktuellen Richtlinien konform ist.

Bericht ″Benutzer″. Ein Bericht, der alle Tivoli Identity Manager-Operationen nach Datum, Anforderer der Operation und Empfänger der angeforderten Operation auflistet.

Bericht ″Datenabgleich″. Ein Bericht, der die Waisenaccounts auflistet, die seit dem letzten Datenabgleich gefunden wurden.

Bericht ″Operation″. Ein Bericht, der die Operationsanforderungen in Tivoli Identity Manager nach

Operationstyp, Operationsdatum, Anforderer der Operation und Empfänger der angeforderten Operation auflistet.

Bericht "Zurückgewiesen". Ein Bericht, der die zurückgewiesenen Anforderungen nach Datum, Anforderer der Operation und Empfänger der angeforderten Operation auflistet.

C

Challenge/Response-Verfahren. Eine Authentifizierungsmethode, die von Benutzern verlangt, auf eine Eingabeaufforderung (Challenge) zu antworten (Response), indem persönliche Informationen zur Verfügung gestellt werden, anhand derer die Identität der Benutzer beim Anmelden am Netzwerk geprüft werden kann.

D

Datenabgleich. Der Prozess, bei dem Informationen des zentralen Datenrepositorys mit dem System des verwalteten Agenten verglichen und eventuelle Abweichungen zwischen beiden Systemen ermittelt werden.

Domänenadministrator. Ein Administrator, der Einrichtungsentitäten, Richtlinien, Services, Arbeitsablaufdefinitionen, Berechtigungsklassen und Benutzer innerhalb der eigenen Verwaltungsdomäne definieren und verwalten kann.

E

Eigner. Eine Person im Tivoli Identity Manager-System, die über einen Account oder einen Service verfügt.

Entität. 1) Eine Person oder ein Objekt, für die bzw. das Informationen gespeichert werden.

2) Eine der folgenden Klassen im Tivoli Identity Manager-System:

- Person
- Geschäftspartnerperson
- Organisation
- Geschäftspartnerorganisation

Eskalationsteilnehmer. Beim Identitätsmanagement eine Person, die berechtigt ist, auf Anforderungen zu antworten, auf die Teilnehmer innerhalb eines für die Eskalation angegebenen Zeitraums nicht antworten. Ein Eskalationsteilnehmer kann als Einzelperson, als Berechtigungsklasse oder durch Verwendung eines angepassten JavaScript-Scripts identifiziert werden.

G

Geschäftspartnerorganisation. Einer der Typen von Tochtergesellschaftsentitäten, die zu einer Organisation hinzugefügt werden können. In der Regel wird eine Geschäftspartnerorganisation zur Identifizierung eines Vertragsnehmers, Lieferanten oder anderer Gruppen von Einzelpersonen verwendet, die keine direkten Mitarbeiter sind, aber Zugriff auf die Ressourcen eines Unternehmens benötigen.

Geschäftspartnerperson. Eine Person in einer Geschäftspartnerorganisation.

H

HR-Mitarbeiterdatenabgleich. Ein automatisierter Vorgang, bei dem das Tivoli Identity Manager-System Benutzerdaten aus einer Datenbank des Personalwesens (HR-Datenbank) oder aus einer derartigen Datei importiert. Siehe auch "DSML-Datenimport".

I

Identitätsrichtlinie. Die Regeln, mit deren Hilfe das Tivoli Identity Manager-System definiert, wie die ID für einen Benutzer erstellt wird.

Inaktiver Account. Ein Account, der im System vorhanden ist, vom Accounteigner jedoch nicht benutzt wird.

Informationsanforderung (RFI). Beim Identitätsmanagement ein Aktionselement, das zusätzliche Informationen von einem angegebenen Teilnehmer anfordert und einen erforderlichen Schritt im Arbeitsablauf (Workflow) darstellt.

K

Kennwort. In der Computer- und Netzwerkabsicherung eine spezifische Zeichenfolge, die vom Benutzer eingegeben und vom System überprüft und authentifiziert wird, wodurch der Benutzer (nach erfolgreicher Authentifizierung) Zugriff auf das System und die dort gespeicherten Informationen erhält.

Kennwortrichtlinie. Die Regeln, die die festgelegten Parameter definieren (wie Länge, zulässige und unzulässige Zeichen), denen alle Kennwörter entsprechen müssen.

O

Organisation. Beim Identitätsmanagement eine Gruppe von Benutzern und Ressourcen, die verhältnismäßig unabhängig sind. Generell können Ressourcen zwar von mehreren Organisationen gemeinsam benutzt werden, doch ist das Maß der Integration zwischen den einzelnen Organisationen relativ gering. Im Allgemeinen stellt eine Organisation ein Unternehmen dar.

Organisationsbaumstruktur. Eine hierarchische Struktur der Organisation, die einen logischen Bereich zum

Erstellen von, Zugreifen auf und Speichern von Organisationsinformationen zur Verfügung stellt.

Organisationseinheit. Eine Gruppe von Benutzern und Ressourcen in einer Organisation, die zum Zweck der Untergliederung einer Organisation in einfacher zu verwaltende Gruppen definiert wird. Benutzer können nur jeweils einer Organisationseinheit zugeordnet werden. Ressourcen werden ebenfalls nur jeweils einer Organisationseinheit zugeordnet, es sei denn, sie werden als global (d.h. für die gesamte Organisation gültig) definiert.

P

Persönliche Informationen. Die persönlichen Informationen eines Benutzers. Diese Informationen können Vor- und Nachnamen, Privatadresse, Telefonnummer, E-Mail-Adresse, Telefonnummer des Büros, den Vorgesetzten usw. einschließen.

Protokollaufzeichnung. Die Aufzeichnung von Transaktionen für ein Computersystem über einen bestimmten Zeitraum.

R

Ressource. Eine Hardware-, Software- oder Datenentität, die von Tivoli-Software verwaltet wird. Siehe auch ″verwaltete Ressource″.

Richtlinie. In Tivoli eine Menge von Regeln, die auf verwaltete Ressourcen angewendet werden. Eine Richtlinie kann beispielsweise für Kennwörter oder für Ressourcen gelten, auf die ein Benutzer zuzugreifen versucht.

Richtliniendurchsetzung. Das Verfahren, das vom Tivoli Identity Manager-System angewendet wird, um den Zugriff durch korrekte Accounts zuzulassen beziehungsweise den Zugriff durch Accounts zu verhindern, die einen Verstoß gegen die gültigen Einrichtungsrichtlinien darstellen.

S

Schlüsselwort. Ein Indexeintrag, der die Richtlinie in einer Suche eindeutig kennzeichnet.

Shared Secret. Ein verschlüsselter Wert, der zum Abrufen des Anfangskennworts eines Benutzers für den Zugriff auf das Tivoli Identity Manager-System verwendet wird. Dieser Wert wird definiert, wenn die persönlichen Informationen des Benutzers erstmals in das System geladen werden.

Standort. Einer der Typen von Tochtergesellschaftsentitäten, die zu einer Organisation hinzugefügt werden können. In der Regel werden Standorte verwendet, um geographische Standorte zum Zwecke des Organisationsmanagements logisch voneinander abzugrenzen.

Stellvertreter. Eine Einzelperson, die für einen anderen Benutzer als Verantwortlicher für die Genehmigung von Anforderungen oder Bereitstellung von Informationen als Reaktion auf Anforderungen bestimmt wurde.

T

Teilnehmer. Beim Identitätsmanagement eine Person, die berechtigt ist, auf Anforderungen zu antworten, die über die Workflow-Engine übergeben werden. Ein Teilnehmer kann als Einzelperson, als Berechtigungsklasse oder durch Verwendung eines angepassten JavaScript-Scripts identifiziert werden.

To-do-Liste. Die Liste der Aktionselemente, die einem Benutzer zugeordnet wurden und von diesem ausgeführt und beendet werden müssen.

U

Unternehmensbereich. Eine Tochtergesellschaftsentität einer Organisation.

V

Verknüpfungsanweisung. Die Menge der Regeln, die definieren, wie Attribute zu handhaben sind, wenn zwei oder mehr Einrichtungsrichtlinien miteinander in Konflikt stehen.

Verzweigung. Jede Ebene innerhalb der Organisationsbaumstruktur wird als Verzweigung bezeichnet. Jeder Verzweigungstyp in der Baumstruktur wird durch ein anderes Symbol gekennzeichnet. Der Inhalt einer Verzweigung mit Untereinheiten kann durch Klicken auf das Pluszeichen (+) neben der Verzweigung angezeigt werden.

Vorgesetzter. Eine Person im Tivoli Identity Manager-System, die als Eigner eines Unternehmensbereichs festgelegt wurde.

W

Wiederherstellen. Das Reaktivieren eines Accounts, der zuvor ausgesetzt wurde.

Z

Zeitlimit bei Eskalation. Der Zeitraum (in Tagen, Stunden, Minuten oder Sekunden), innerhalb dessen ein Teilnehmer auf eine Anforderung antworten muss, bevor es zur Eskalation kommt.

Zugriff. Die Berechtigung für die Nutzung von auf Computersystemen gespeicherten Informationen oder Daten.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Marken

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken der International Business Machines Corporation:

AIX
DB2
IBM
IBM Logo
OS/390
SecureWay
Tivoli
Tivoli-Logo
Universal Database
WebSphere
z/OS
zSeries

Lotus ist in gewissen Ländern eine eingetragene Marke der Lotus Development Corporation und/oder IBM Corporation.

Domino ist in gewissen Ländern eine Marke der International Business Machines Corporation und der Lotus Development Corporation.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Java und alle Java-basierten Marken und Logos sind in gewissen Ländern Marken oder eingetragene Marken von Sun Microsystems, Inc.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Java und alle Java-basierten Marken und Logos sind in gewissen Ländern Marken oder eingetragene Marken von Sun Microsystems, Inc.

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

Index

A

Account
  Bericht
    Beschreibung 26
Account, Bericht
  Beschreibung 36
  generieren 37
Accounts
  ändern 15
  aussetzen 16
  Einrichtung zurücknehmen 16
  hinzufügen 14
  Kennwort abrufen 5
  verwalten 13
  wiederherstellen 16
Ad-hoc
  Bericht
    Beschreibung 26
Ad-hoc-Bericht
  Beschreibung 38
  generieren 38
Allgemeine Funktionen
  Gültigkeitsdatum 10
  Navigation
    Methoden 9
    Navigationsleiste des Hauptmenüs 9
    Taskleiste 9
  Onlinehilfe 10
Anmeldung
  Kennwort vergessen 6
  Routine 5
Anstehende Anforderungen
  Beschreibung 20
Ausgangsposition
  Accountverwaltung
    Accounts aussetzen 16
    Accounts wiederherstellen 16
    Beschreibung 13
    Einrichtung von Accounts zurücknehmen 16
    neue Accounts hinzufügen 14
    vorhandene Accounts ändern 15
  anstehende Anforderungen
    Beschreibung 20
  beendete Anforderungen
    Beschreibung 20
  Berechtigung delegieren
    Beschreibung 22
    Stellvertreter ändern 23
    Stellvertreter hinzufügen 22
    Stellvertreter wechseln 22
  Funktionsbereiche 11
  Kennwort
    Kennwortprüffragen des Challenge/Response-Verfahrens ändern 23
    Verwaltung 11
  Kennwörter ändern 17
  persönliche Informationen
    Beschreibung 20
  To-do-Liste
    Anforderungsdetails anzeigen 19
    Beschreibung 18

B

Beendete Anforderungen
  anzeigen 20
  Beschreibung 20
Benutzer
  Bericht
    Beschreibung 26, 31
    generieren 32
Benutzerschnittstelle
  Navigation
    Navigationsleiste des Hauptmenüs 9
    Taskleiste 9
Berechtigung delegieren
  ändern 22
  Beschreibung 22
  hinzufügen 22
Bericht
  Account
    Beschreibung 26, 36
    generieren 37
  Ad-hoc
    Beschreibung 26, 38
    generieren 38
  Benutzer
    Beschreibung 26, 31
    generieren 32
  Datenabgleich
    Beschreibung 26, 34
    generieren 34
  Operation
    Beschreibung 25, 27
    generieren 28
  Ruhend
    Beschreibung 26, 35
    generieren 35
  Service
    Beschreibung 25, 29
    generieren 30
  Typen
    Account 26, 36
    Ad-hoc 26, 38
    Benutzer 26, 31
    Datenabgleich 26, 34
    Operation 25, 27
    Ruhend 26, 35
    Service 25, 29
    Zurückgewiesen 26, 33
  verfügbare Typen 25
  Zurückgewiesen
    Beschreibung 26, 33
    generieren 33

D

Datenabgleich
  Bericht
    Beschreibung 26, 34
    generieren 34
Dokumente
  Onlinezugriff vi

G

Gültigkeitsdatum 10

K

Kennwort
- Challenge/Response-Verfahren
  - Antworten 7, 23
  - Funktion 7
- vergessen
  - anmelden 6
  - Antworten auf Kennwortprüffragen des Challenge/Response-Verfahrens konfigurieren 23
- verwalten 11

M

Mitarbeiter
- Firmeninformationen 21
  - Nummer 21
  - Postadresse 21
  - Sekretär/in 21
  - Titel 21
  - Vorgesetzter 21
  - Zimmernummer 21
- Kontaktinformationen
  - Aliasnamen 21
  - E-Mail-Adresse 21
  - Mobiltelefonnummer 21
  - Pagernummer 21
  - Telefonnummer (Büro) 21
  - Telefonnummer (privat) 21
- persönliche Informationen
  - Initialen 21
  - Nachname 21
  - Organisationsberechtigungsklassen 21
  - Privatadresse 21
  - Shared Secret 21
  - vollständiger Name 21
  - Vorname 21

Monospaceschrift vii

N

Navigation
- Methoden 9
- Navigationsleiste des Hauptmenüs 9
- Taskleiste 9

Navigationsleiste des Hauptmenüs 9

O

Onlinehilfe 10
Operation, Bericht
- Beschreibung 25, 27
- generieren 28

P

Persönliche Informationen 20
- ändern 22
- Firmeninformationen, Registerkarte
  - Personalnummer 21
  - Postadresse 21

Persönliche Informationen *(Forts.)*
- Firmeninformationen, Registerkarte *(Forts.)*
  - Sekretär/in 21
  - Titel 21
  - Vorgesetzter 21
  - Zimmernummer 21
- hinzufügen 22
- Kontaktinformationen, Registerkarte
  - Aliasnamen 21
  - E-Mail-Adresse 21
  - Mobiltelefonnummer 21
  - Pagernummer 21
  - Telefonnummer 21
  - Telefonnummer (privat) 21
- Persönliche Informationen, Registerkarte
  - Initialen 21
  - Nachname 21
  - Organisationsberechtigungsklassen 21
  - Privatadresse 21
  - Shared Secret 21
  - Vollständiger Name 21
  - Vorname 21

Publikationen
- Onlinezugriff vi

R

Richtliniendurchsetzung
- Konformitätsmarkierung
  - Fragezeichen 14
  - konform 13
  - nicht konform 14
  - Warnung 14

Ruhend
- Bericht
  - Beschreibung 26

Ruhend, Bericht
- Beschreibung 35
- generieren 35

S

Service
- Bericht
  - Beschreibung 25, 29
  - generieren 30

Shared Secret 21

T

Taskleiste 9
Text, fett gedruckt vii
Text, kursiv vii
To-do-Liste
- Beschreibung 18
- Details anzeigen 19
- sortieren 19

V

Verwalten
- Accounts 13
- Kennwort 11

Z

Zielgruppe v
Zurückgewiesen
  Bericht
    Beschreibung 26
Zurückgewiesen, Bericht
  Beschreibung 33
  generieren 33

Programmnummer: 5724-C34

SC12-3276-00